1. PASSWORD MACHINE B/S MANAGEMENT SYSTEM OPERATION DETAILS

1.1. System Login

Login

Default login url：https://192.168.20.20:8443.

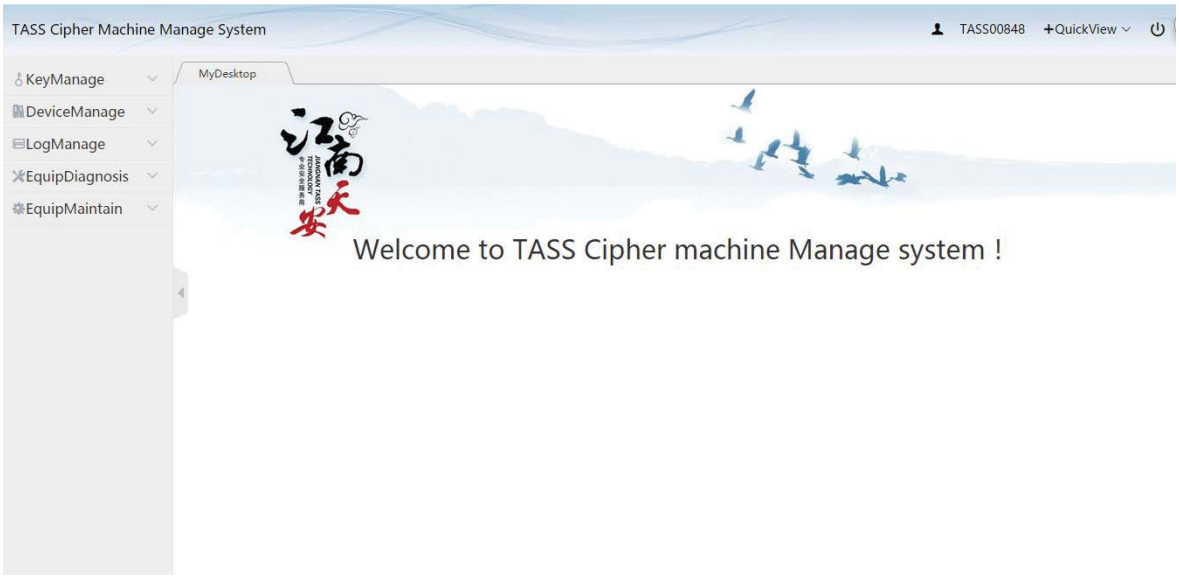
To insert UKEY, select the UKEY to log in, enter the UKEY password, click the "login" button to login, and the page condition has the following qualifies:

1、 UKEY: must be an administrator UKEY.

2、 UKEY password: must fill.

Note: for unregistered UKEY users, click the "register" button to register for UKEY.

1.2. The Home Page



The home page

After logging in, it will jump to the front page of the system.

Users can operate according to the system menu, the top right corner of the homepage.

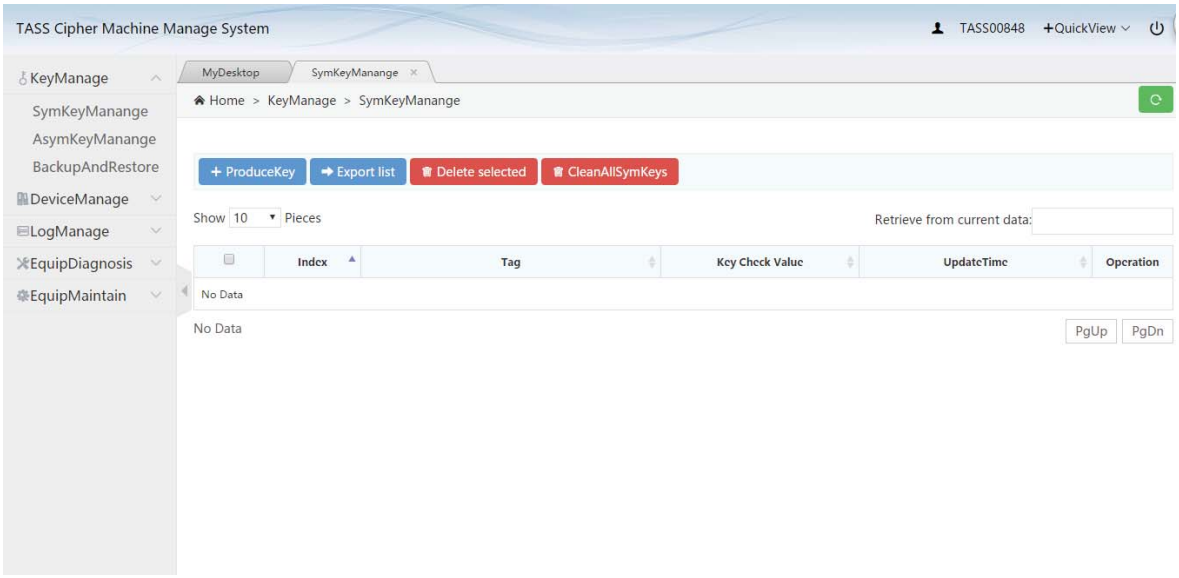
[UKEY serial number], which can be managed by UKEY;

Direct access to "network configuration", "trusted client management", "error code query" and other operational pages;

Click the [Exit] button, you can exit the system;

1.3. Key Management

1.3.1. Symmetric Key Management

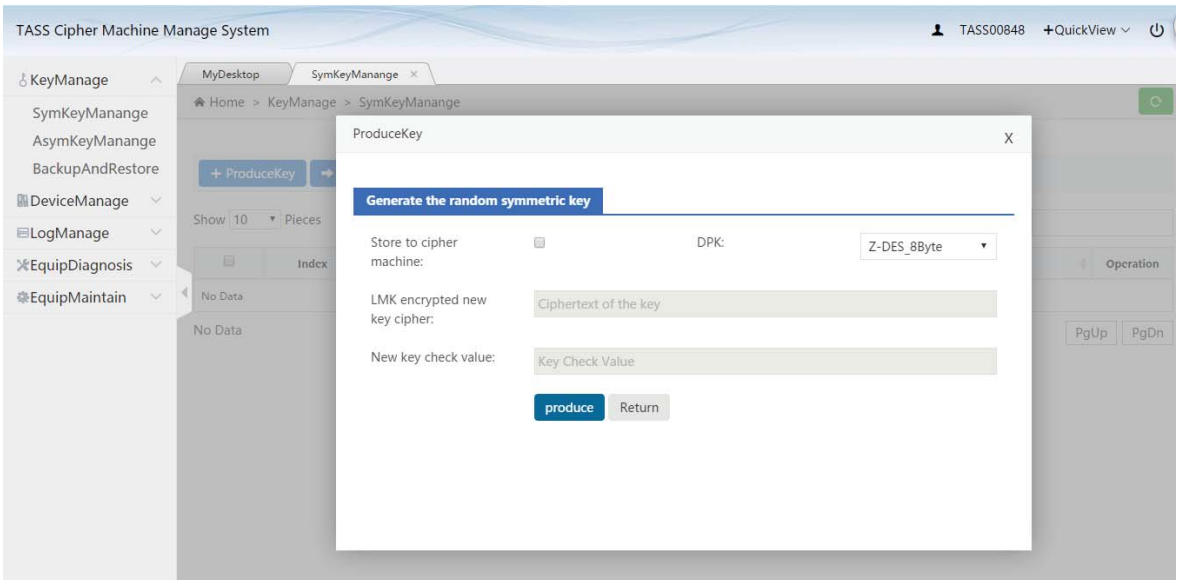


Symmetric key list

A symmetric key list is the basic information about the existing key and the display of the executable operation.

1.3.1.1. Generate The Key

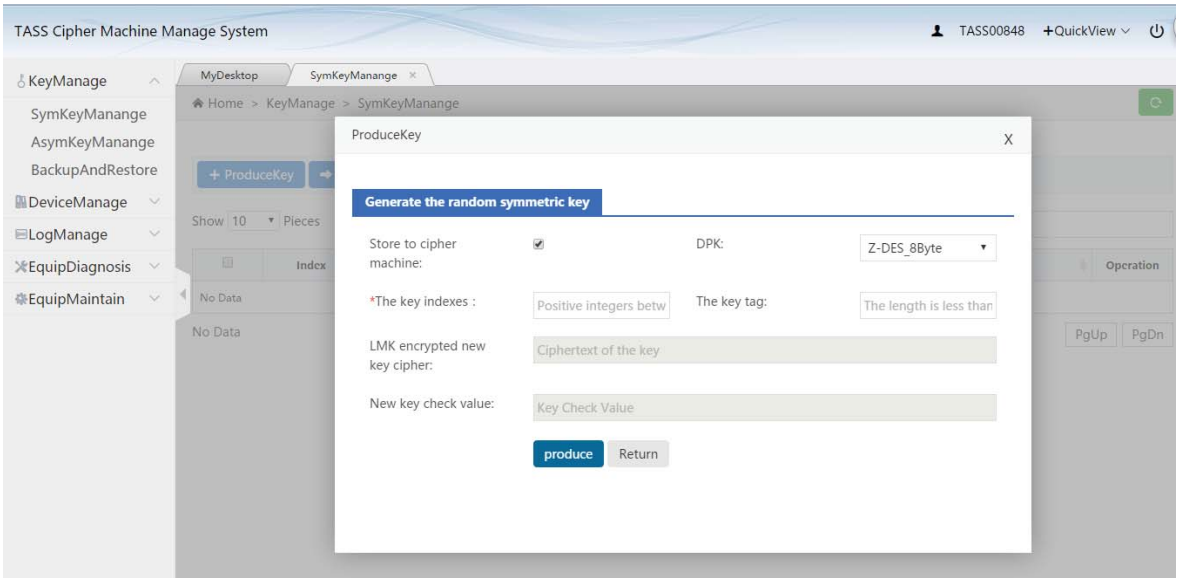
Method one: Only produce, do not store to cipher machine



Produces non-stored symmetric secret keys

1. Stored in a cipher machine: no.
2. Algorithm id: optional;
3. LMK encrypted new key message: click "generate" button to display;
4. New key check value: click "generate" button to display;

Method two: store to the password machine after production



Generate the stored symmetric secret key

1. Stored in a cipher machine: must be chosen;
2. Algorithm id: optional;
3. Key index: must be completed;
4. Key label: refill;
5. LMK encrypted new key message: click "generate" button to display;
6. New key check value: click "generate" button to display;

When generated, click the "return" button or "X" in the upper right corner, and the newly created key will appear in the list of symmetric keys.

1.3.1.2. Export The List

After clicking the "export list" button, the symmetric key list is exported to Excel.

1.3.1.3. Delete

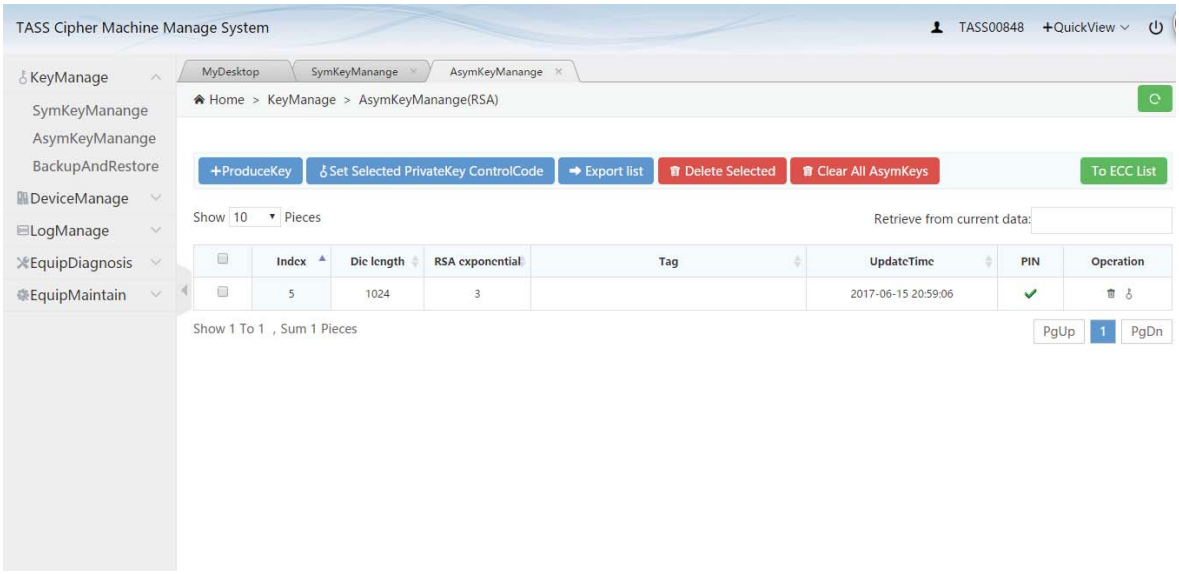
Click "delete" button or "delete" icon to execute symmetric key delete.

1.3.1.4. Clear All The Keys

Click "clear all key" button to execute all symmetric secret key removal operations.

1.3.2. Asymmetric Key Management

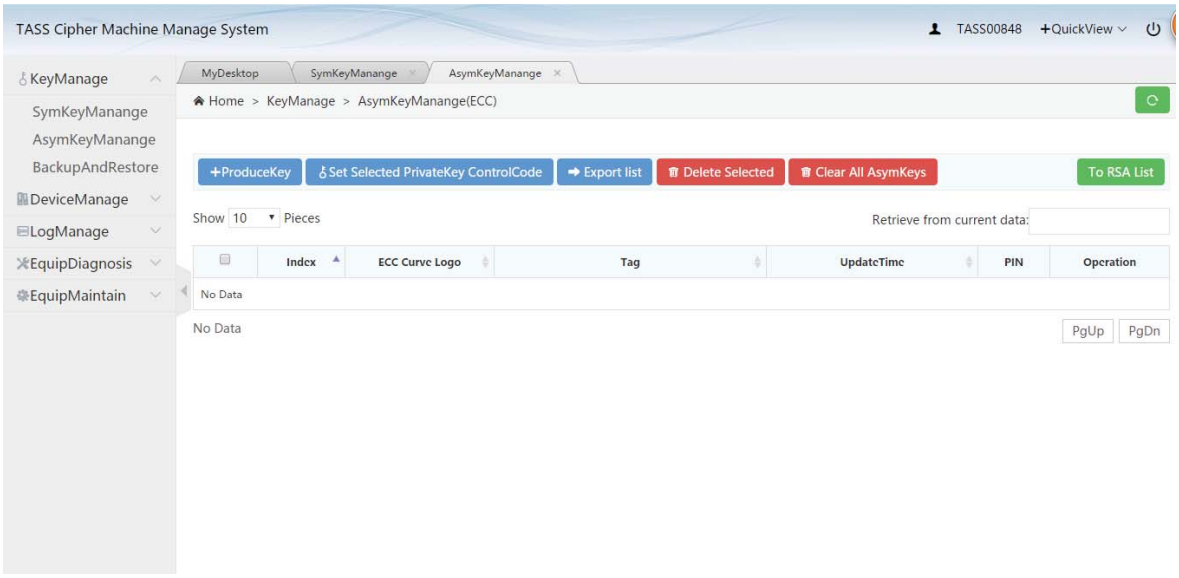
1.3.2.1. RSA Key List



RSA Asymmetric key list

The RSA asymmetric key list is the basic information that currently produces the RSA key and the display of executable operations.

1.3.2.2. ECC Key List

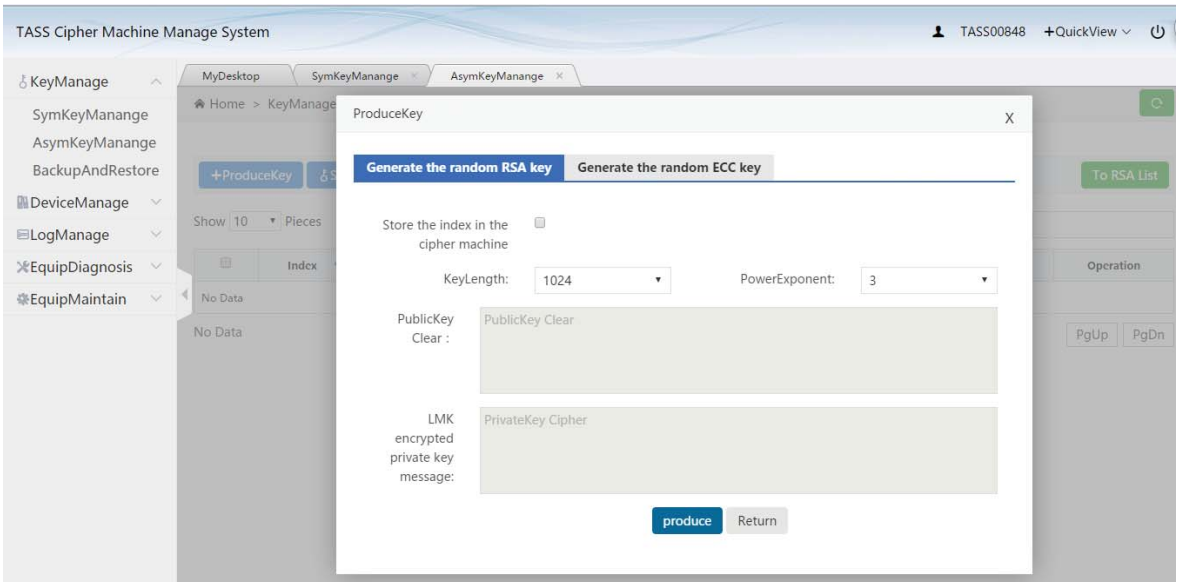


ECC Asymmetric key list

The ECC asymmetric key list is the basic information that currently produces the ECC key, as well as the display of executable operations.

1.3.2.3. Generate The Key - Generate The Random RSA Key

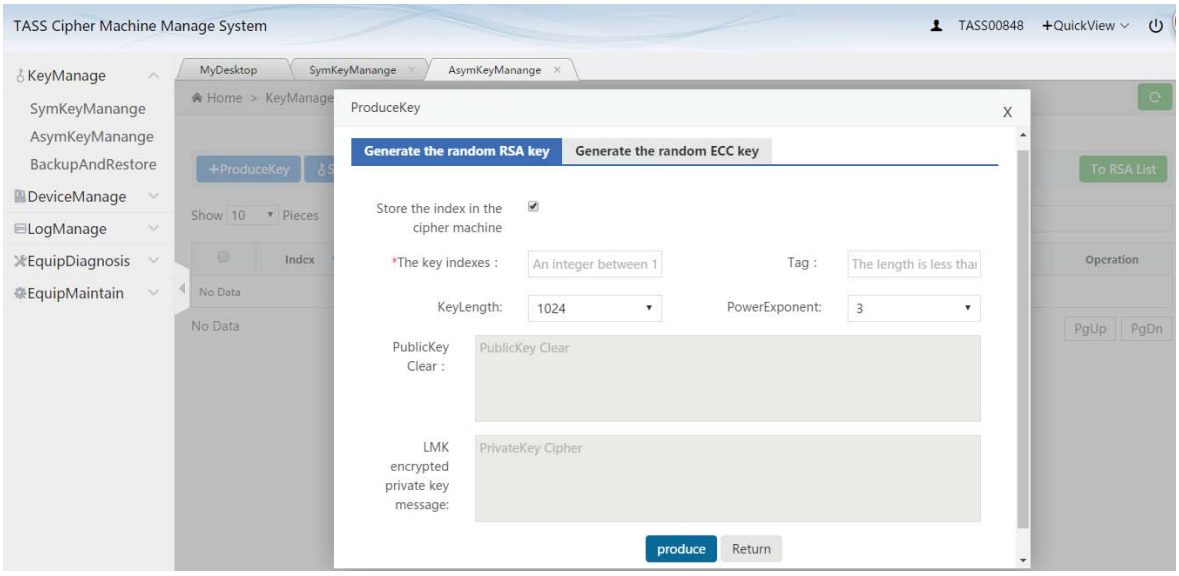
Method one: only produce, do not store to cipher machine



Generates non-stored RSA keys

1. Stored in a cipher machine: no.
2. Key module: optional;
3. Power index: optional;
4. Public key text: click "generate" button to display;
5. LMK encrypted private key message: click "generate" button to display;

Method two: store to the password machine after production



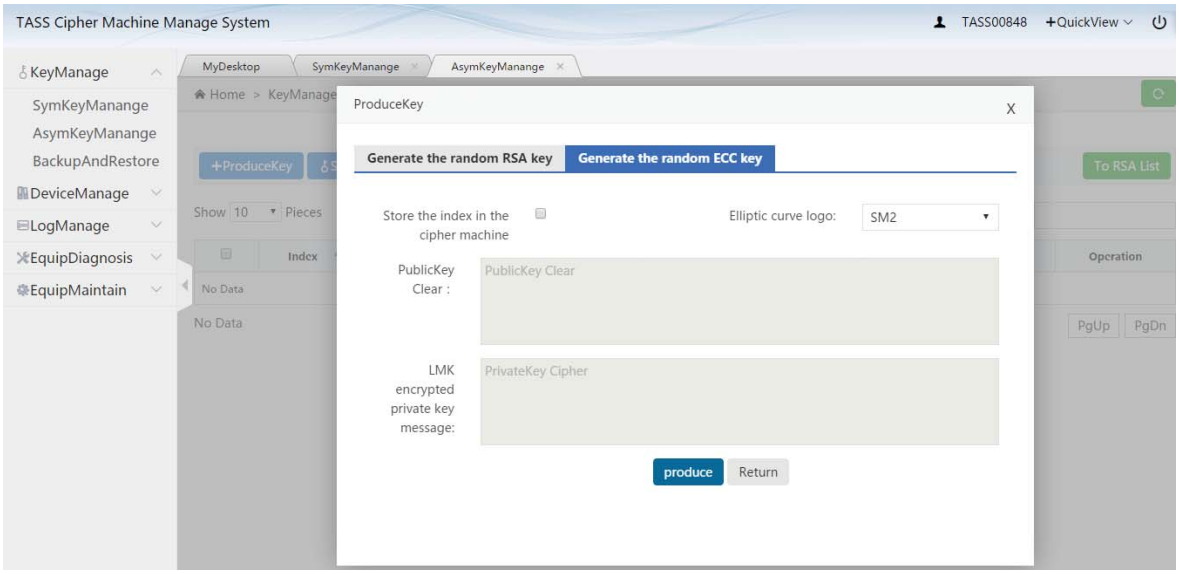
Generate the storage RSA key

1. Stored in a cipher machine: must be chosen;
2. Key index: must be completed;
3. Key label: refill;
4. Key module: optional;
5. Power index: optional;
6. Public key text: click "generate" button to display;
7. LMK encrypted private key message: click "generate" button to display;

When generated, click the "return" button or "X" in the upper-right corner, and the new key will be displayed in the RSA unsymmetric key list.

1.3.2.4. Generate The Key - Generate The Random ECC Key

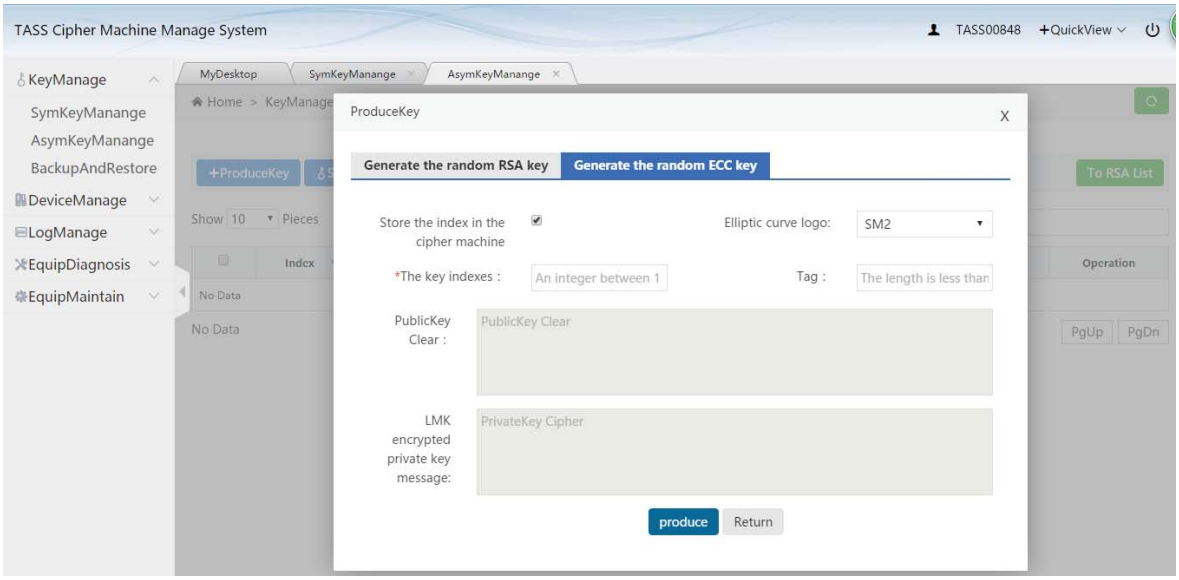
Method one: only produce, do not store to cipher machine



Generate non-stored ECC keys

1. Storage to cipher machine: no.
2. Elliptic curve id: optional;
3. Public key text: click "generate" button to display;
4. LMK encrypted private key message: click "generate" button to display;

Method two: store to the password machine after production



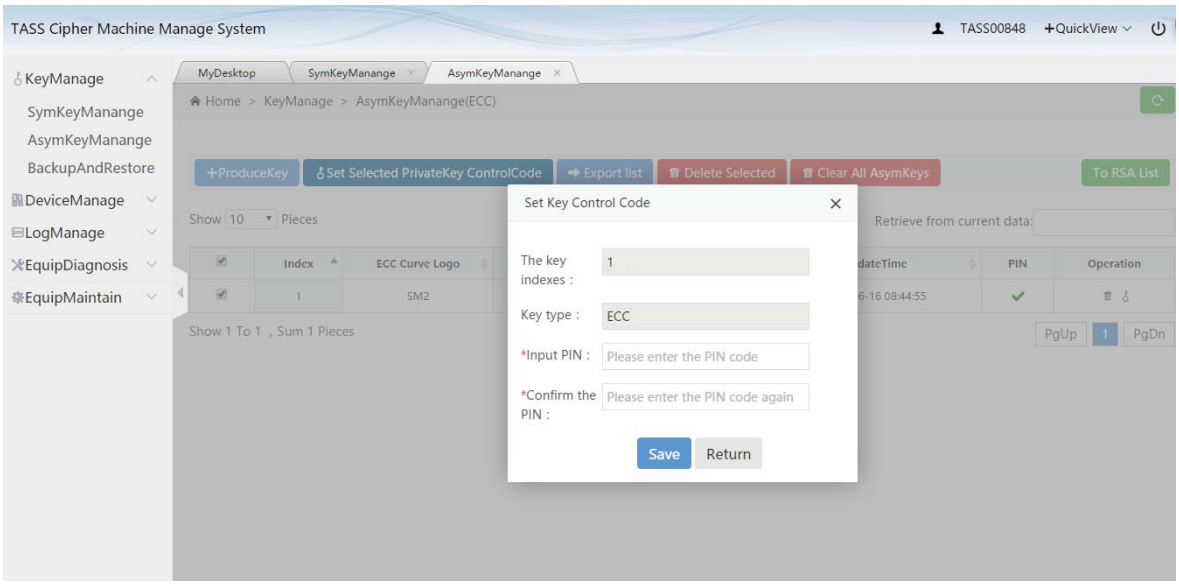
Generate the stored ECC key

1. Store to cipher machine: must choose;
2. Elliptic curve id: optional;
3. Key index: must be completed;
4. Key label: refillable;
5. Public key text: click "generate" button to display;
6. LMK encrypted private key message: click "generate" button to display;

When generated, click the "return" button or "X" in the upper right, and the new key will appear in the ECC asymmetric key list.

1.3.2.5. Set The Private Key Control Code

Click "set the private key control code" button or icon to set the private key control code for multiple or single keys.



Set the private key control code

Enter the same PIN code twice, click save, and set the success.

1.3.2.6. The Export List

After clicking the "export list" button, the asymmetric key list is exported to Excel.

1.3.2.7. Delete

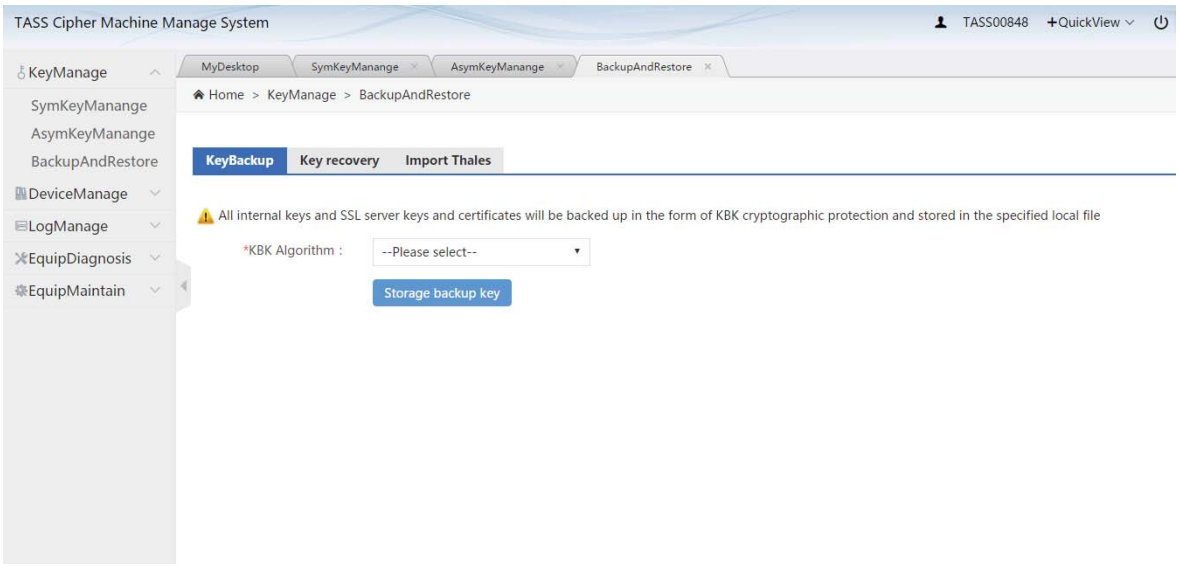
Click "delete" button or "delete" icon to perform asymmetric key deletion.

1.3.2.8. Clear all keys

Click the "clear all key" button to execute all non-symmetric secret key removal operations.

1.3.3. Backup And Restore

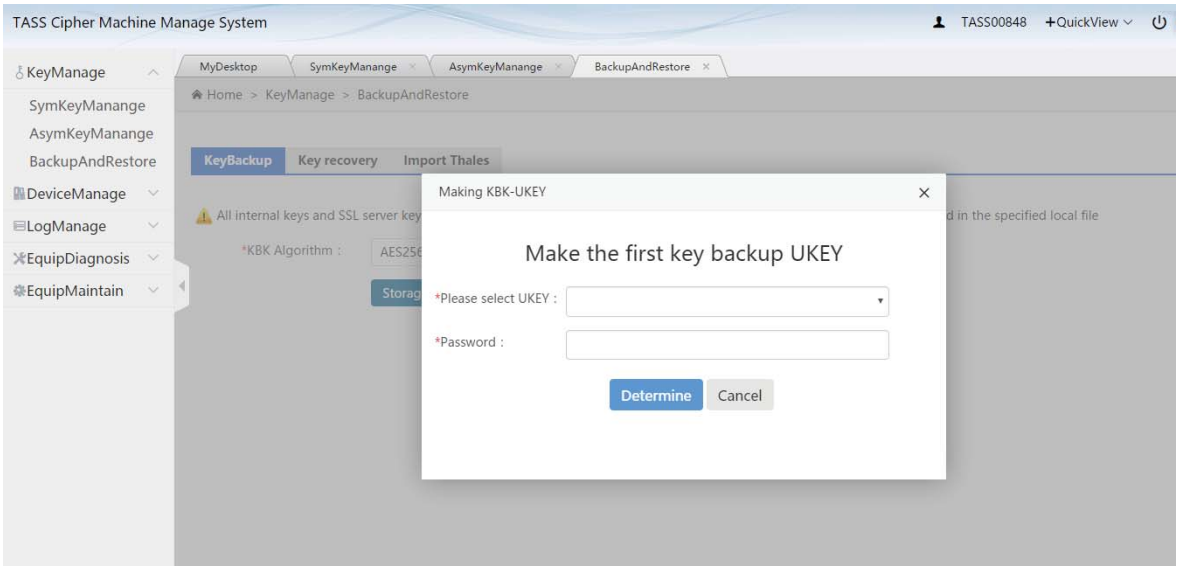
1.3.3.1. Key Backup



Key backup

Select the KBK algorithm: select (SM4, ASE256).

Click on "save the backup key", first make the key backup UKEY, as shown below:

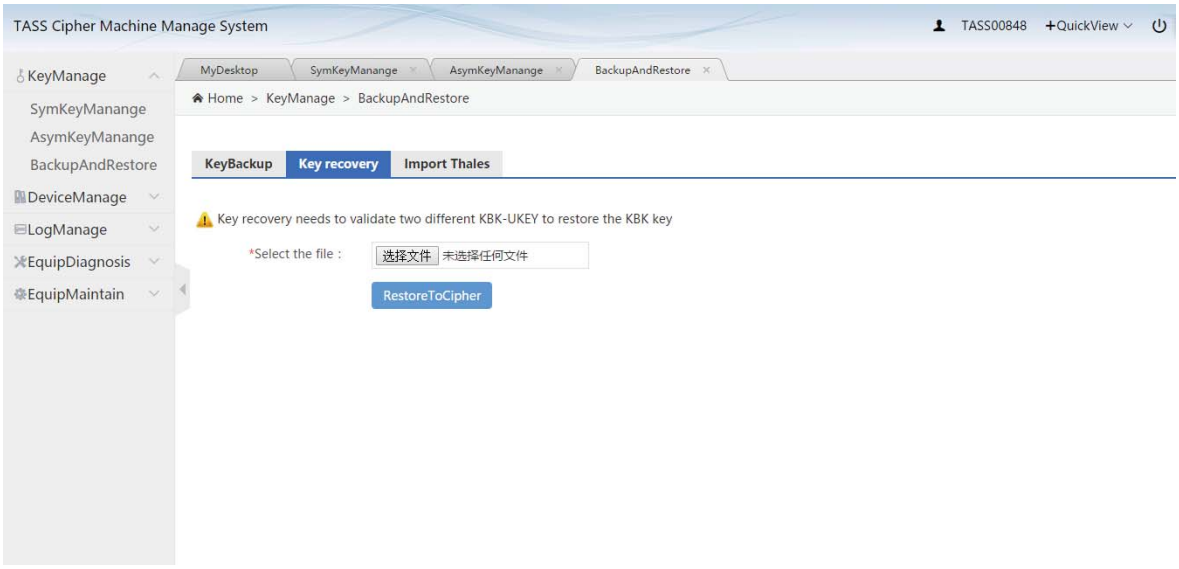


Make the key backup UKEY

1. Please select UKEY.
2. UKEY password: must be filled;

Note: you need to make three key backup ukeys;

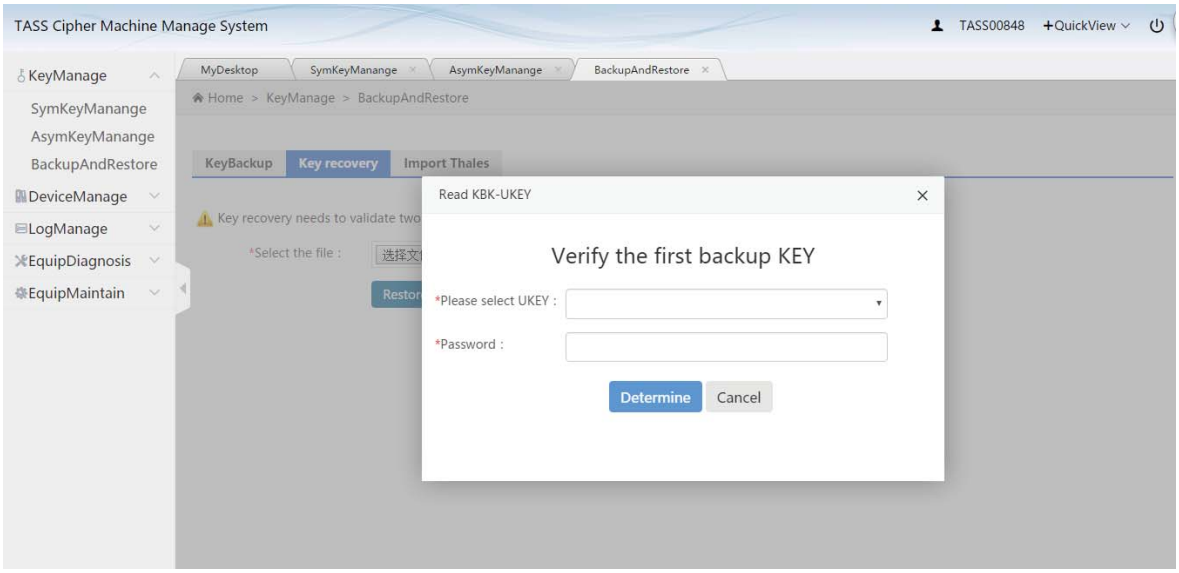
1.3.3.2. Key Recovry



Key recovry

Select file: select (dat form of key file).

Click restore import to cipher machine, first to verify the key backup UKEY, as shown below:



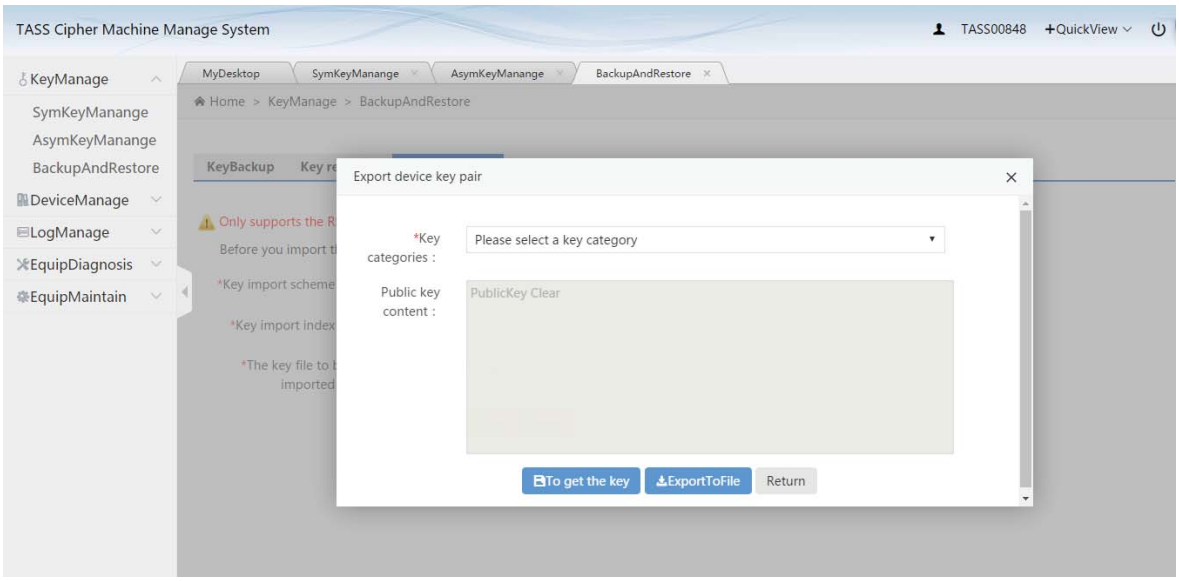
Verify the key backup UKEY

1. Please select UKEY.
2. UKEY password: must be filled;

Note: you need to validate three key backup ukeys;

1.3.3.3. Key Import

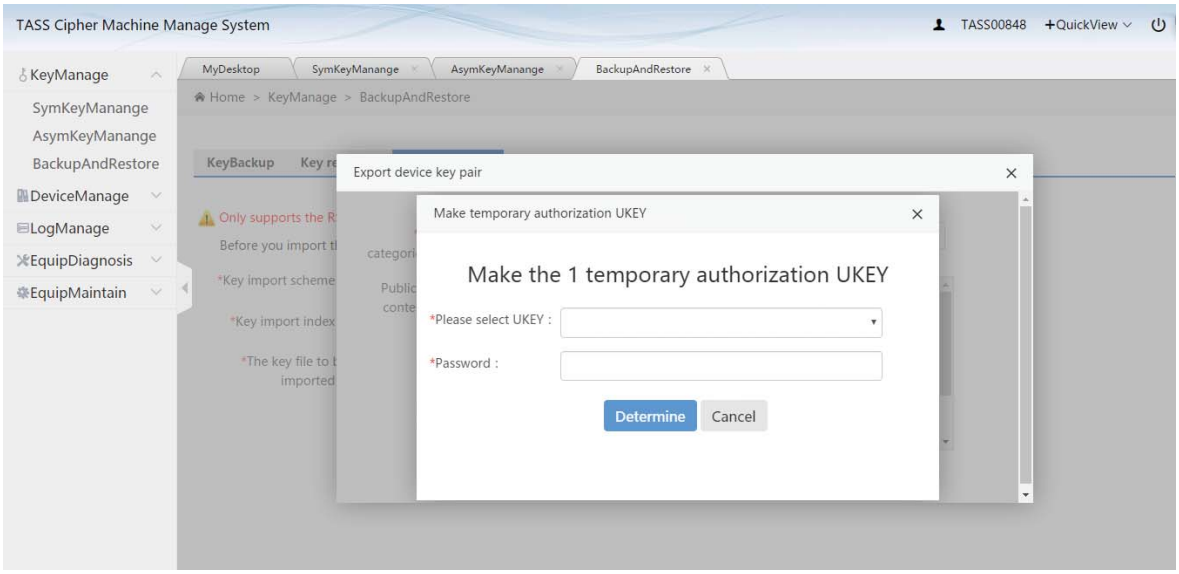
You need to confirm that you have exported the device key pair, as shown below:



Export device key pair

Key category: optional.

1. Click "get the key", and the public key content will display the public key in plain text.
2. Click "export to the file", first to make a temporary authorization UKEY, as shown below:

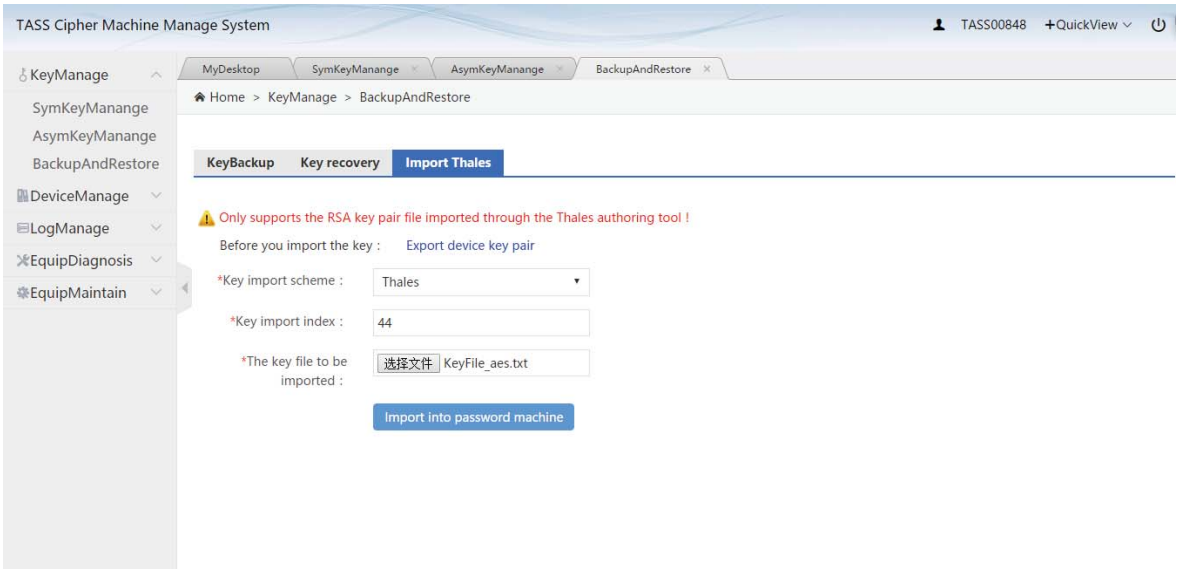


Verify the key backup UKEY

1. Please select UKEY.
2. UKEY password: must be filled;

Note: you need to make 3 temporary authorization UKEY to complete the production and select export.

Key import



Key import

Note: this support only supports the import RSA type of.txt key file.

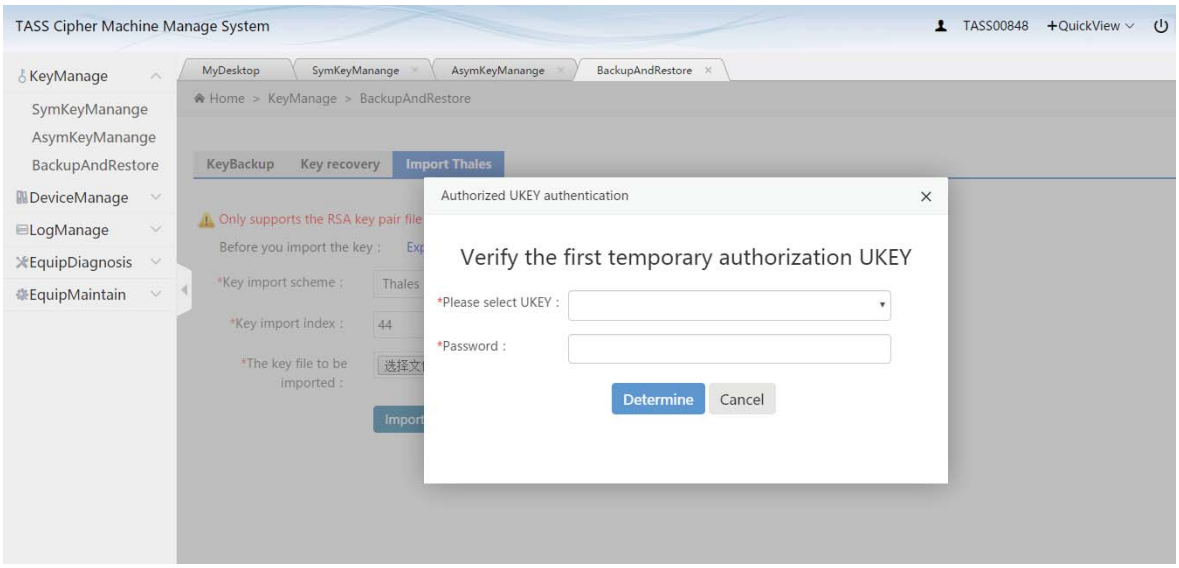
1. Key import solution: (Thales);
2. Key indexes to be imported: mandatory;
3. Key files to be imported: the selected (TXT form key file produced by the Thales production tool);

The details are as follows:

One. Management tools.rar is an import equipment key tool
Objective: to verify the correctness of the decryption process using the customer's key, and import the user's private key into the cipher machine as the device key.
Steps:
1. Modify the IP in tacipher.ini
2. Double-click the importkey_2_4096.exe
3. Enter 2, then press enter.
4. Execute service /tmp/setdev.sh //if not, put it in the service /tmp directory, chmod u + x/tmp/setdev.sh and then execute.

Two. Apple.rar is an imported thales tool
1.Select rsa device key / / purpose: make temporary authorization ukey
2. Select indexes, files in this directory, and import keys.

Click "import to the password machine", first to verify the temporary authorization UKEY, as shown below:



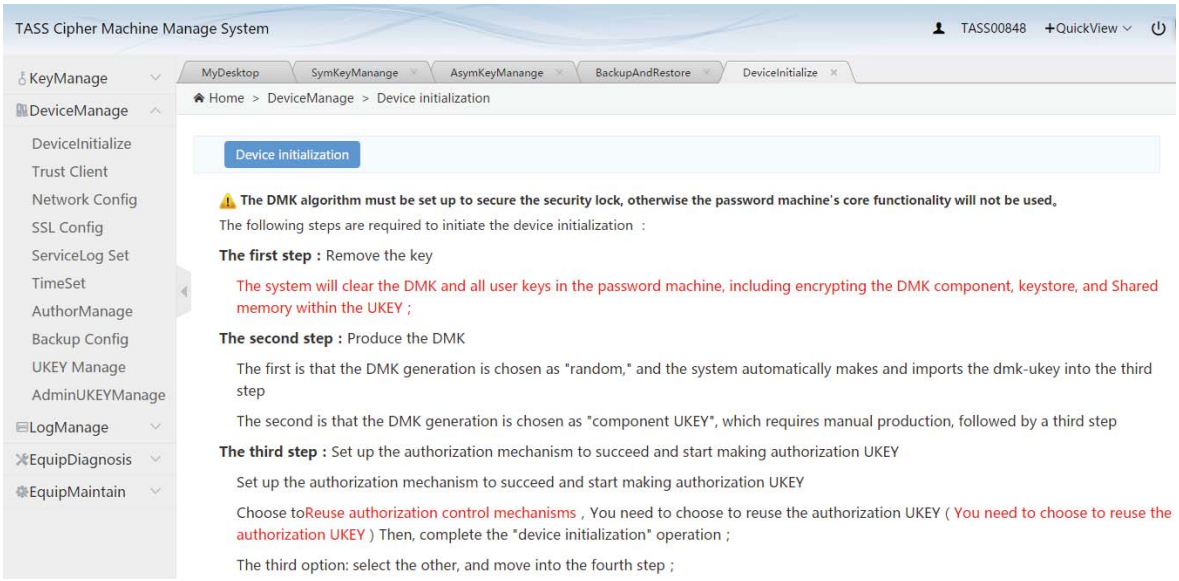
Verify the temporary authorization UKEY

1. Please select UKEY.
2. UKEY password: must be filled;

Note: you need to verify three temporary authorization UKEY;

1.4. Equipment Management

1.4.1. Equipment Initialize



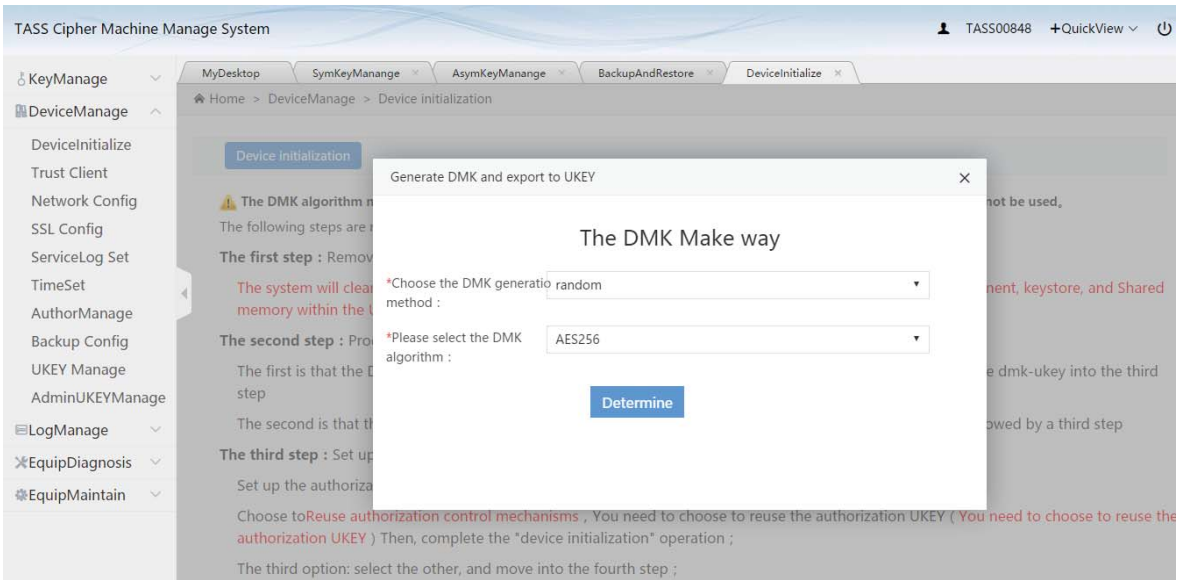
Equipment initialize

Note: prior to this, you need to set the security state lock to the security state, otherwise you will not be able to initialize the device.

Step 1: click the "ok" system to give the prompt and automate the removal of the key;

Step 2: generate the DMK:

One, produce random DMK

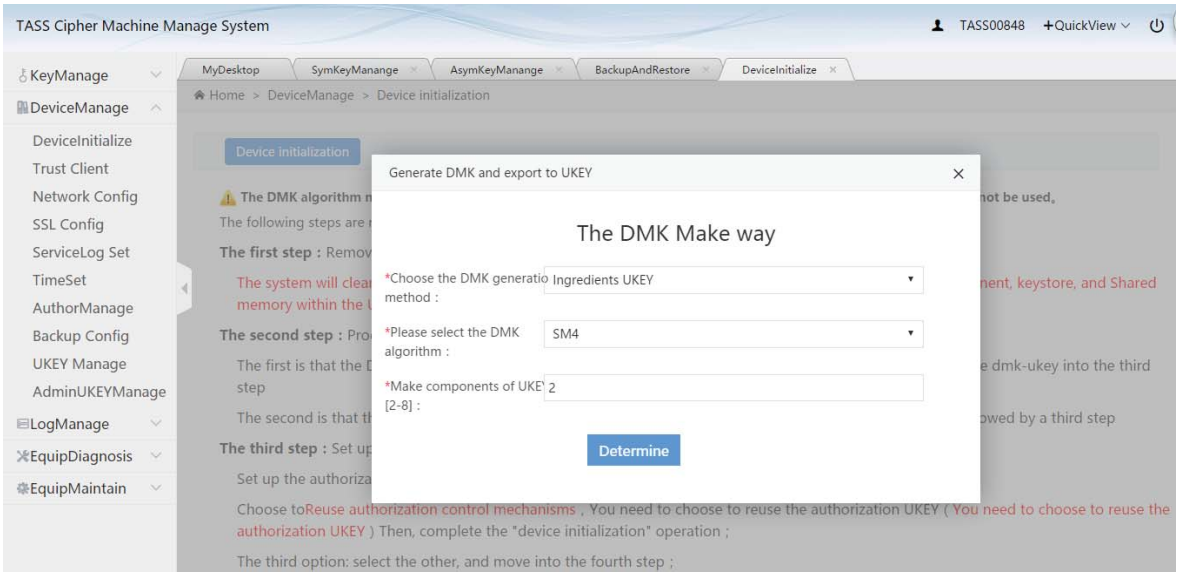


Device initialization - random

1. Choose the DMK algorithm: (SM4, AES256, 3DES192);
2. Choose the DMK method: (random);

Note: the DMK generation is chosen as "random", click "ok", the system will be automatically made, and the dmk-ukey will be imported directly into the third step.

Two, produce the constituent card DMK

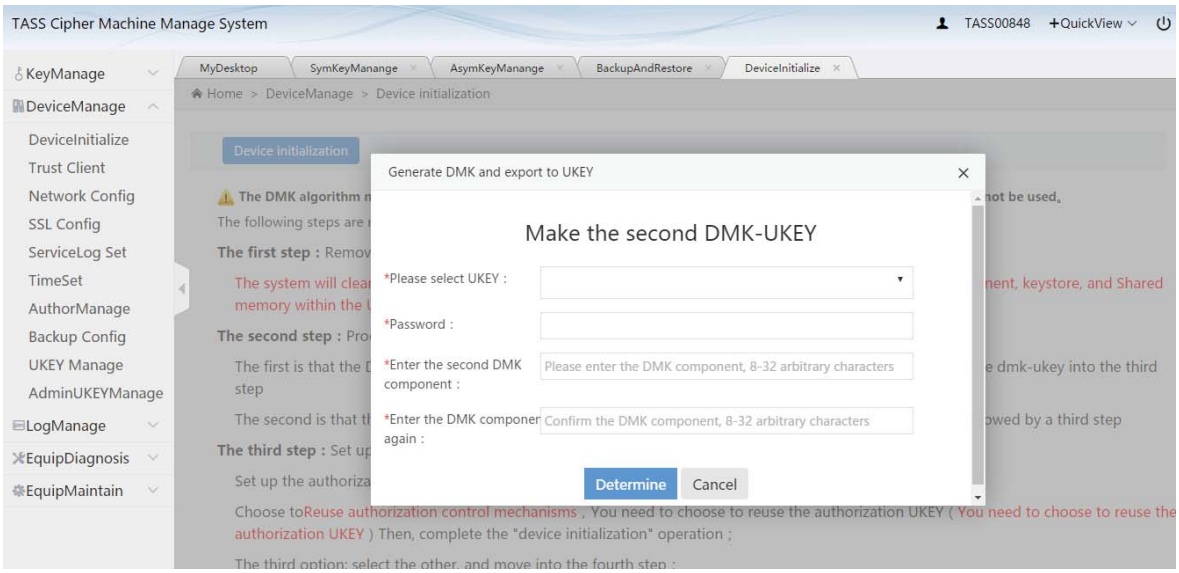


Device initialization - component UKEY

1. Choose the DMK algorithm: (SM4, AES256, 3DES192);
2. Please select the DMK generation mode: (component UKEY);
3. The number of components to be made: must be filled (2 ~ 8);

Note: the DMK generation option is "component UKEY", which requires manual production, importing the dmk-ukey and then entering the third step.

One, making the DMK - UKEY

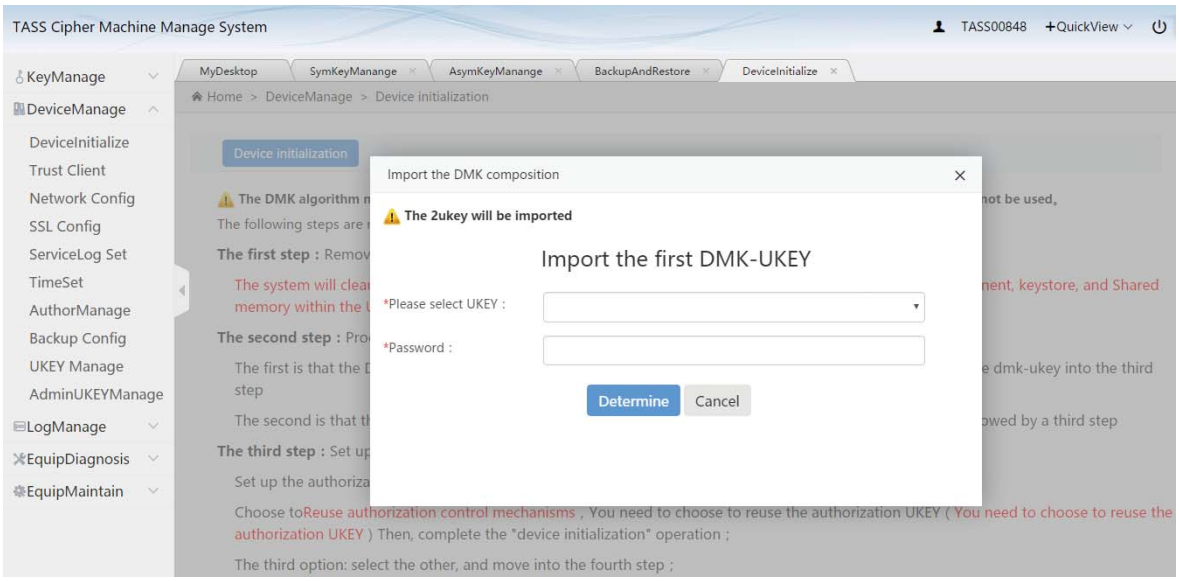


Making the DMK - UKEY

1. Please select UKEY.
2. UKEY password: must be filled;
3. Please enter the n DMK component.
4. Enter the n DMK component again.

When finished, import the dmk-ukey.

Two, import the DMK - UKEY

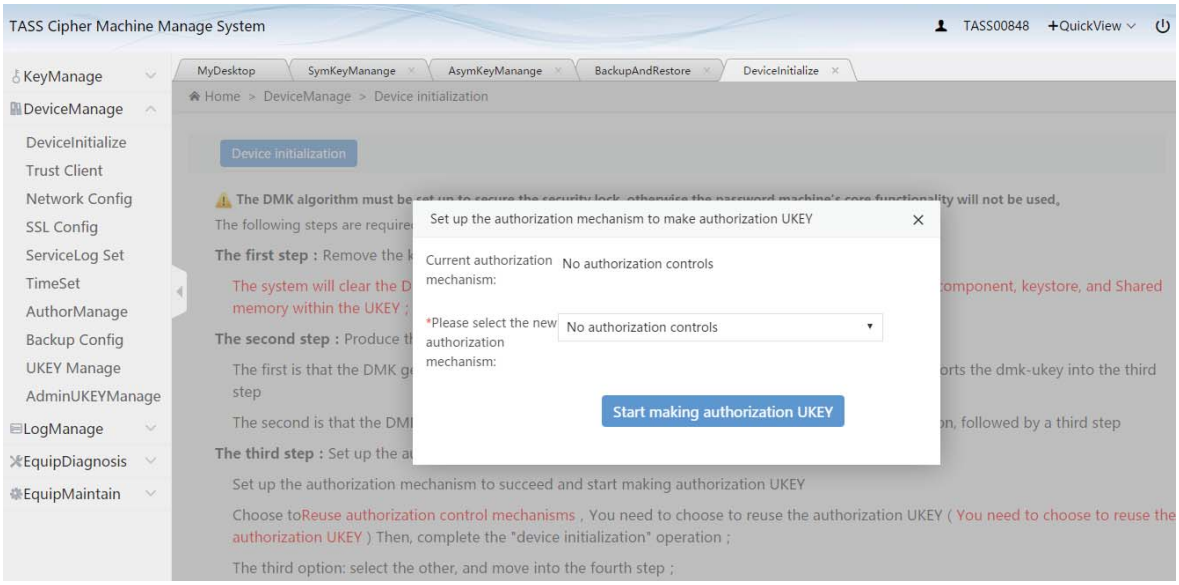


Import the DMK - UKEY

1. Please select UKEY.
2. UKEY password: must be filled;

When you complete the import, enter the third step.

Step 3: set up the authorization mechanism:



Set up authorization mechanism

The current authorization mechanism: this shows the authorization mechanism in [authorization management];

Please select the new authorization mechanism: (

No authorization control mechanism: no authorization UKEY is required;

Select 1 authorization control mechanism: create 1 authorization UKEY to verify 1 authorization UKEY;

Select 2 authorization control mechanism: make 3 authorization UKEY to verify 2 authorization UKEY;

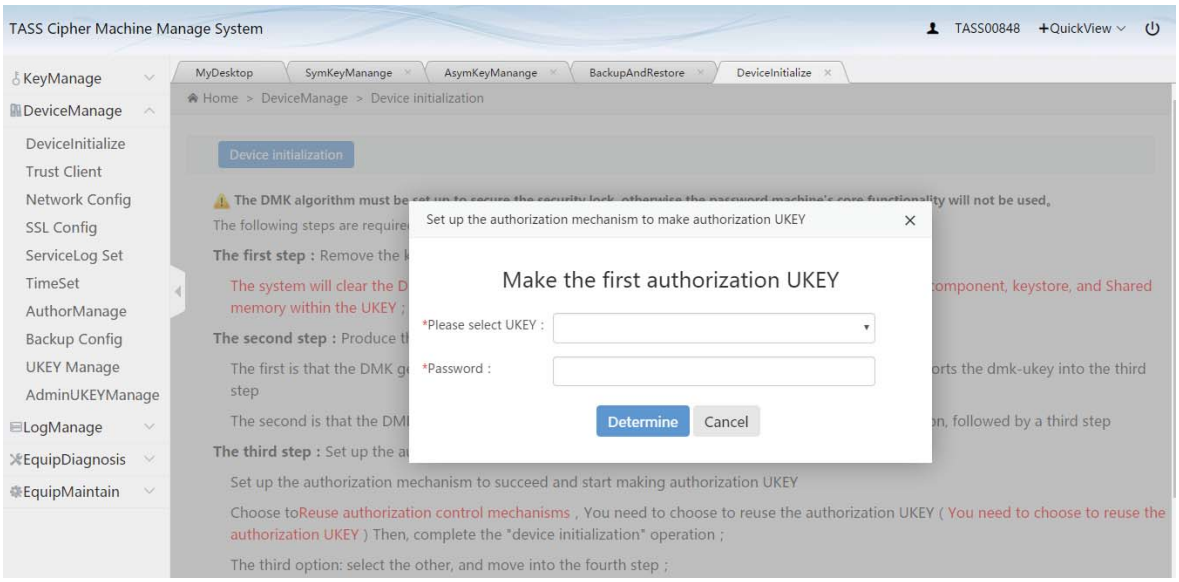
Select 3 authorization control mechanism: make 5 authorization UKEY to verify 3 authorization UKEY;

Reuse authorization control mechanism: select a UKEY that has been created by other machines to authorize UKEY)

Click on "start making authorization UKEY" or "reuse authorization UKEY" to move into the fourth step.

Step 4:

First one: making authorization UKEY

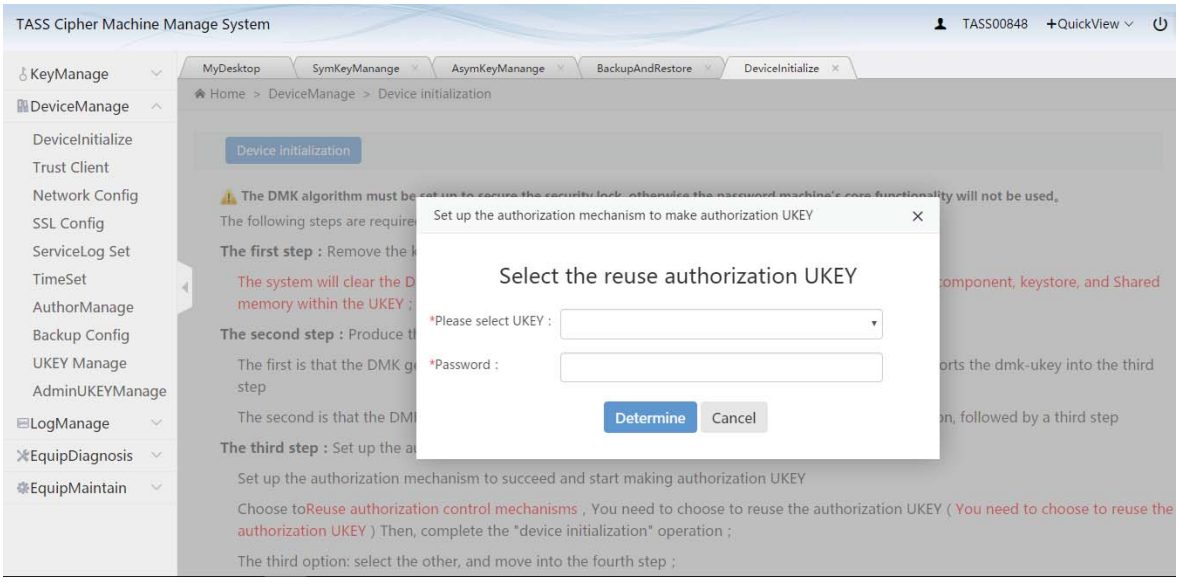


Set up the authorization UKEY

1. Please select UKEY.
2. UKEY password: must be filled;

Completion of equipment initialization after completion of production;

Second one: reuse authorization UKEY



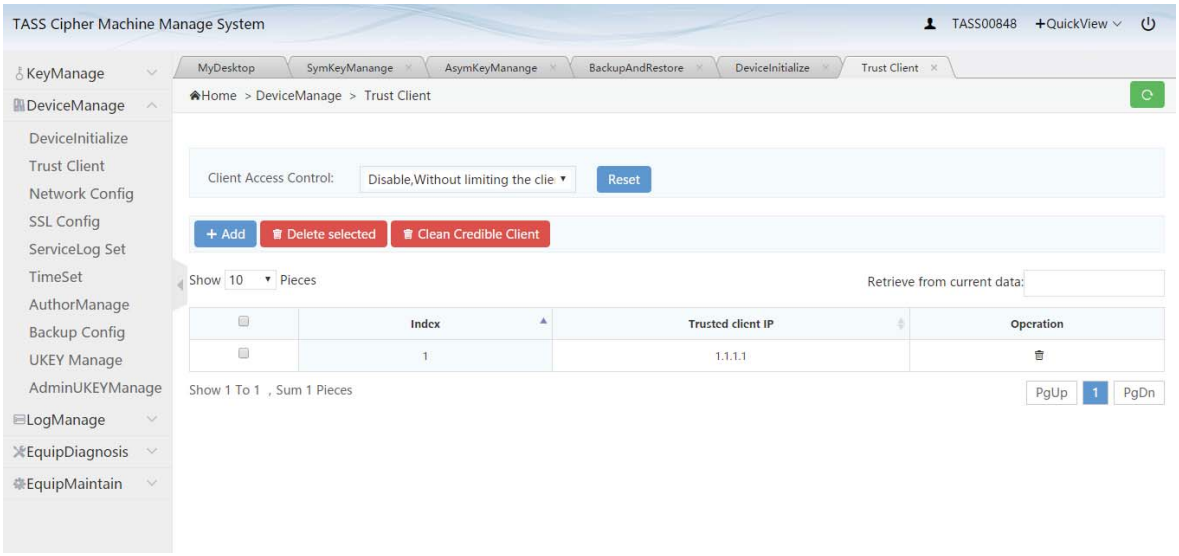
Reuse authorized UKEY

1. Choose UKEY: (UKEY, which has been authorized by other machines);

2. UKEY password: must be filled;

When the reuse is complete, the device initialization is done;

1.4.2. Trusted Client Management



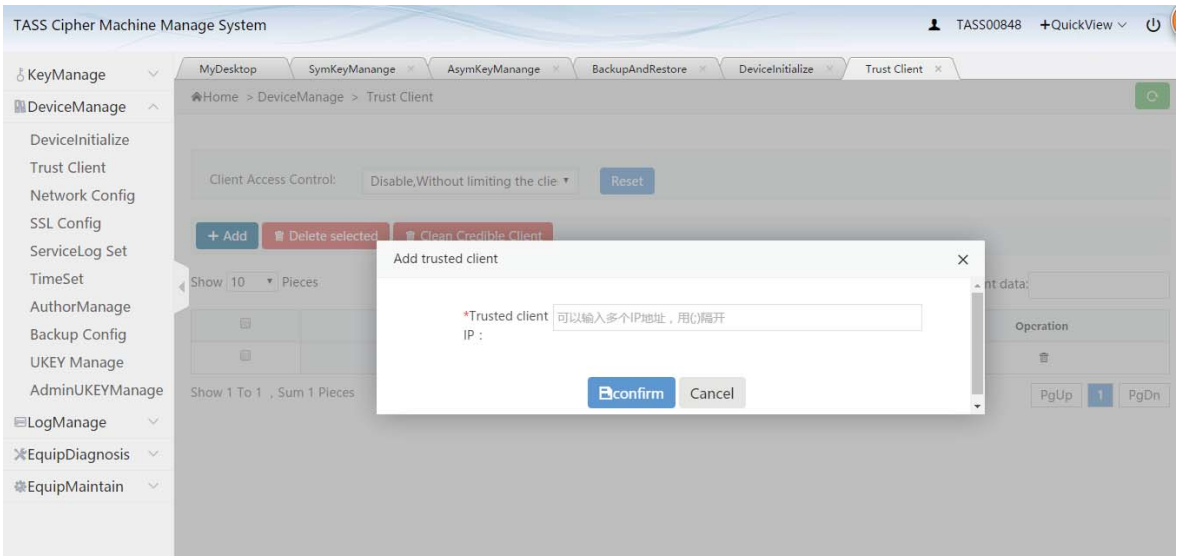
Trusted client list

Trusted client management is the basic information about the trusted client that is currently created and the display of executable operations.

1.4.2.1. Reset

Client access control: optional, click "reset" button to reset.

1.4.2.2. Add



Trusted client add

Trusted client Ip: must be filled (in batches, in "; ");

1.4.2.3. Delete

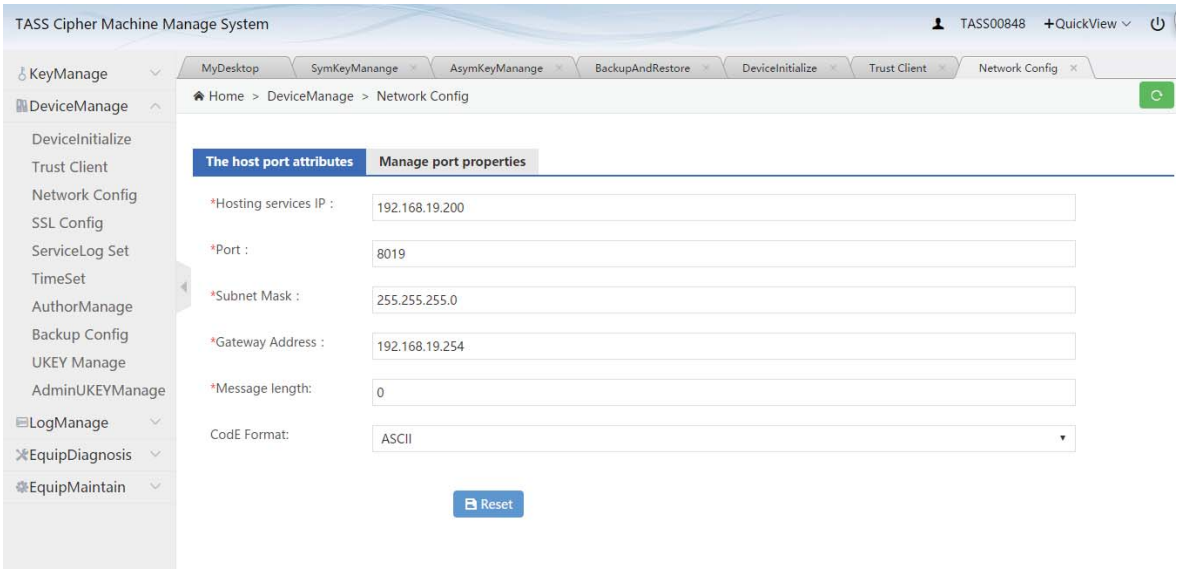
Click the "batch delete" button or "delete" icon to execute the trusted client delete operation.

1.4.2.4. Clear The Trusted Client

Click the "clear trusted client" button to execute the trusted client cleanup operation.

1.4.3. Network Configuration

1.4.3.1. Host Port Attribute



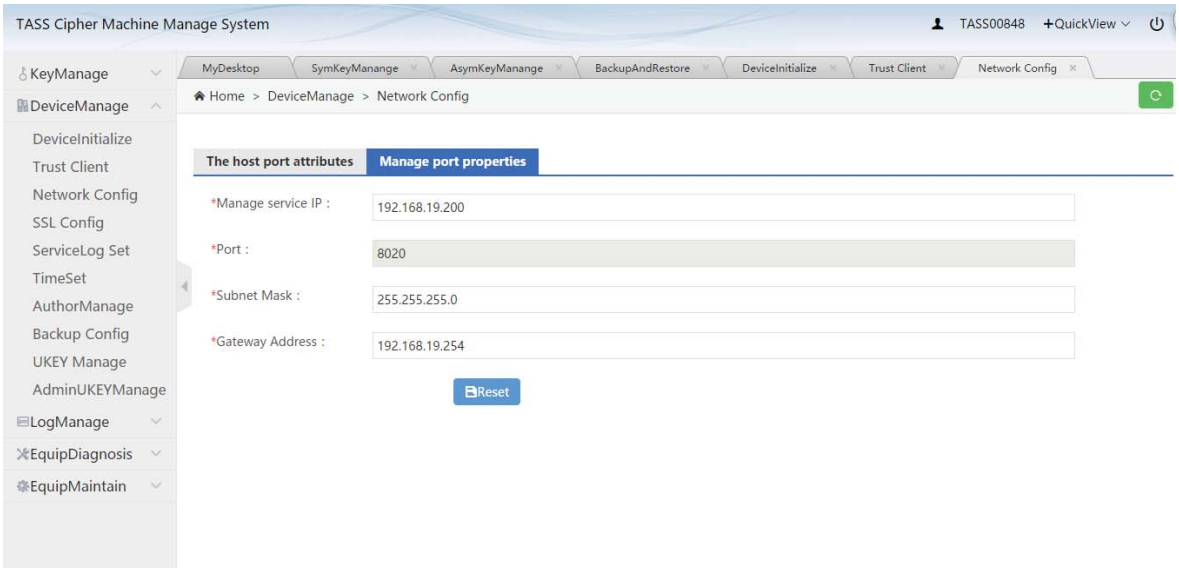
Host port attribute

This configuration can be reset, and the main operations are as follows:

1. Host service IP: resetting;
2. Port number: resets;
3. Subnet mask: resetting;
4. Gateway address: reset;
5. Message header length: resets;
6. Message insulation encoding format: resetting;

Note: after this operation, you need to restart the host service to take effect.

1.4.3.2. Manage Port Properties



Manage port properties

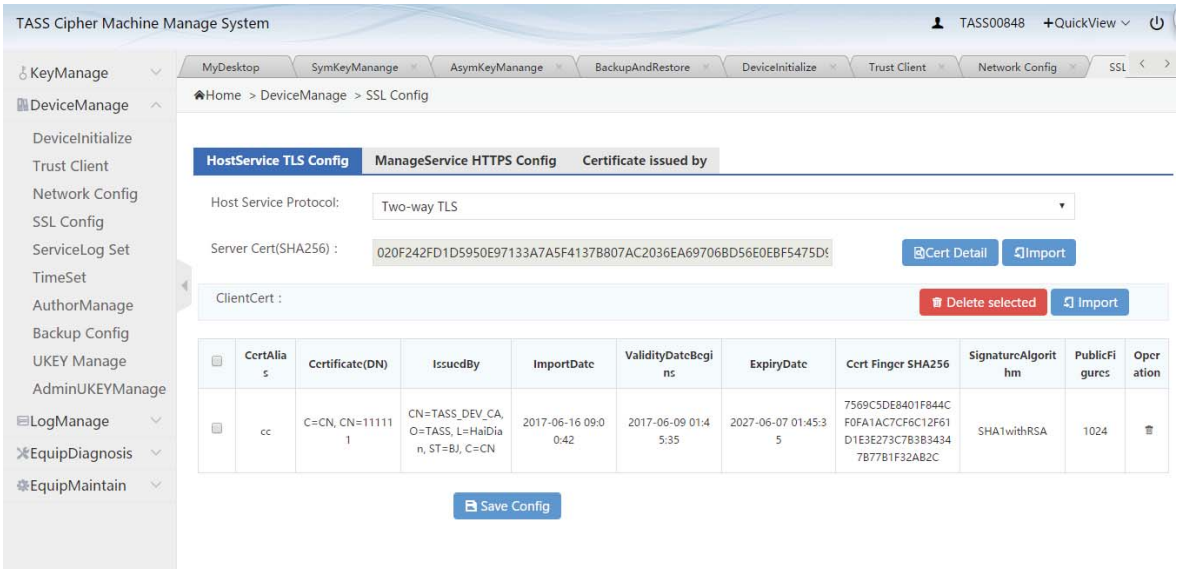
This configuration can be reset, and the main operations are as follows:

1. Management service IP: resets;
2. Port number: resets;
3. Subnet mask: resetting;
4. Gateway address: reset;

Note: after this operation, you need to restart the host service to take effect.

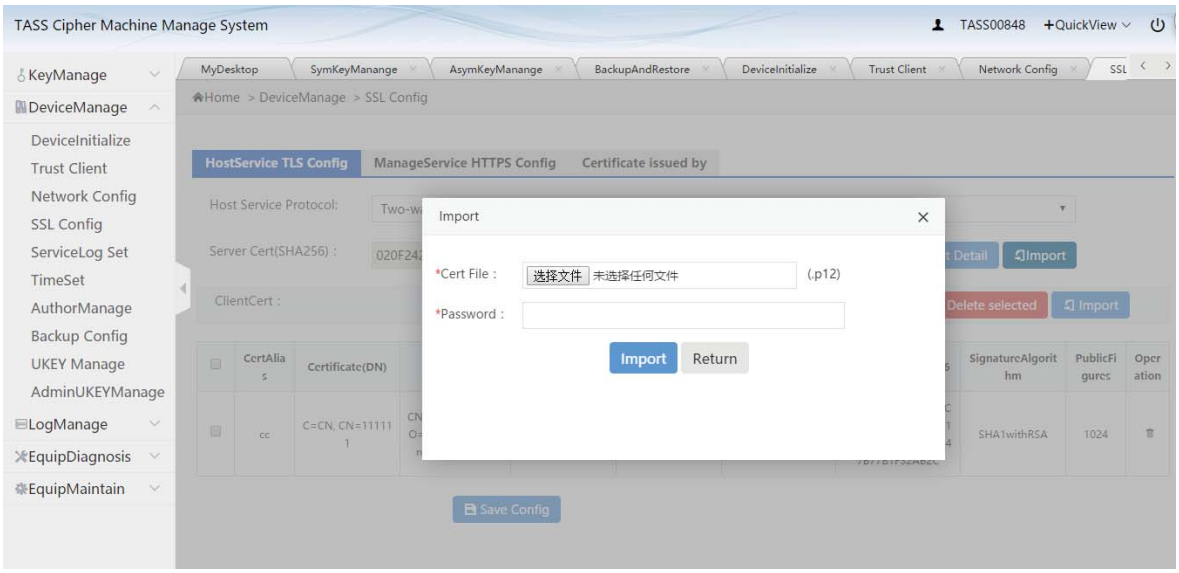
1.4.4. SSL Configuration Management

1.4.4.1. Host Service TLS Configuration



Host service TLS configuration

One. Import updates (service side certificates)

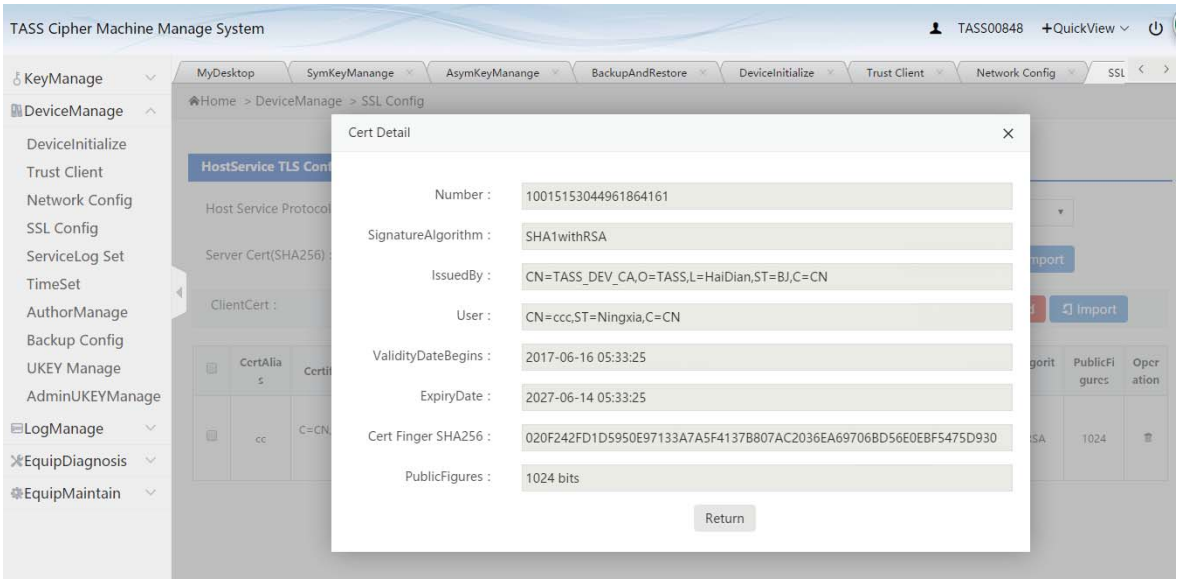


Import updates (service side certificates)

1. Certificate file: optional (p12 form certificate file);
2. Certificate private key: must be completed;

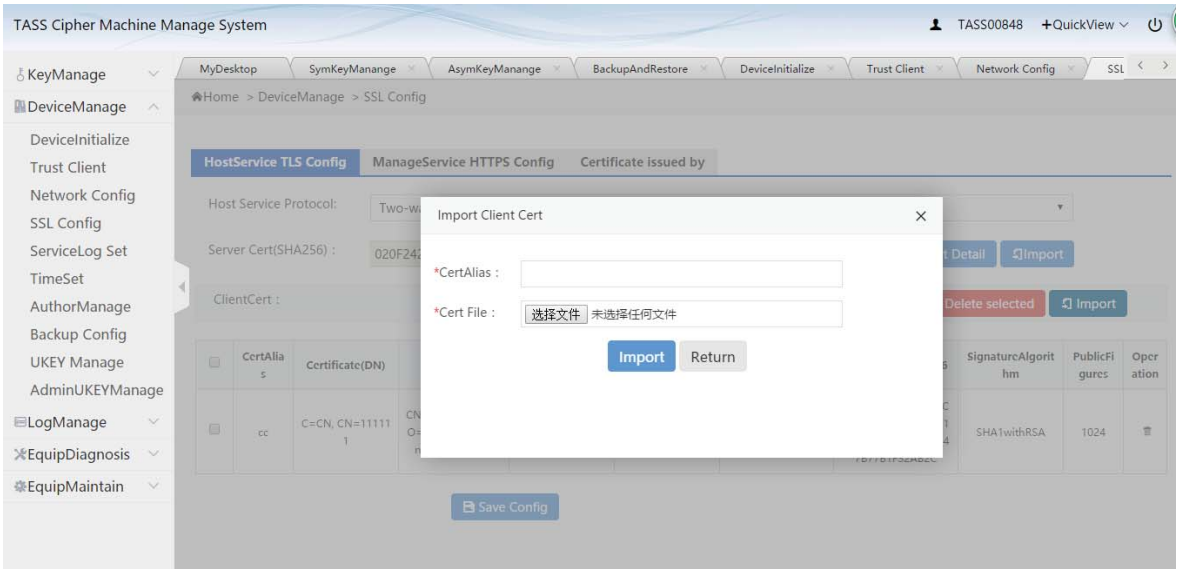
Note: after this operation is completed, the password machine should be restarted.

Two. Certificate details (client certificate)



Certificate details (service side certificates)

Three. Import (client certificate)



Import (client certificate)

1. Certificate alias: mandatory.
2. Certificate file: optional (certificate file in cer form);

Four. Delete (client certificate)

Click "delete" button or "delete" icon to execute client certificate delete.

Five. Save config

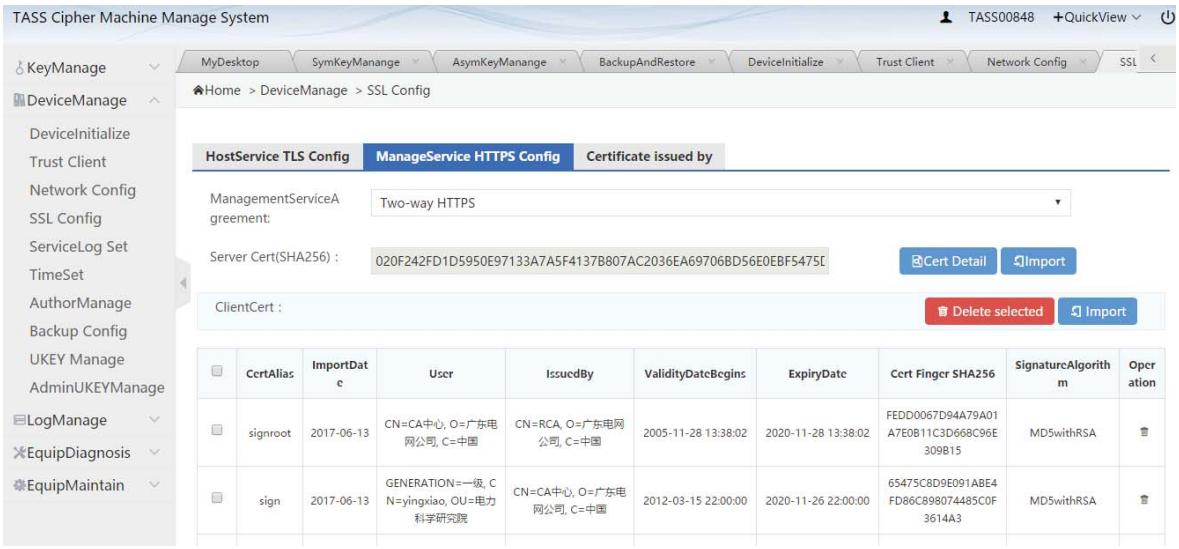
Host service protocol: optional（

Express communication: you can choose directly and save the configuration.

One-way TLS: failure to save the configuration if there is no service end certificate in the device;

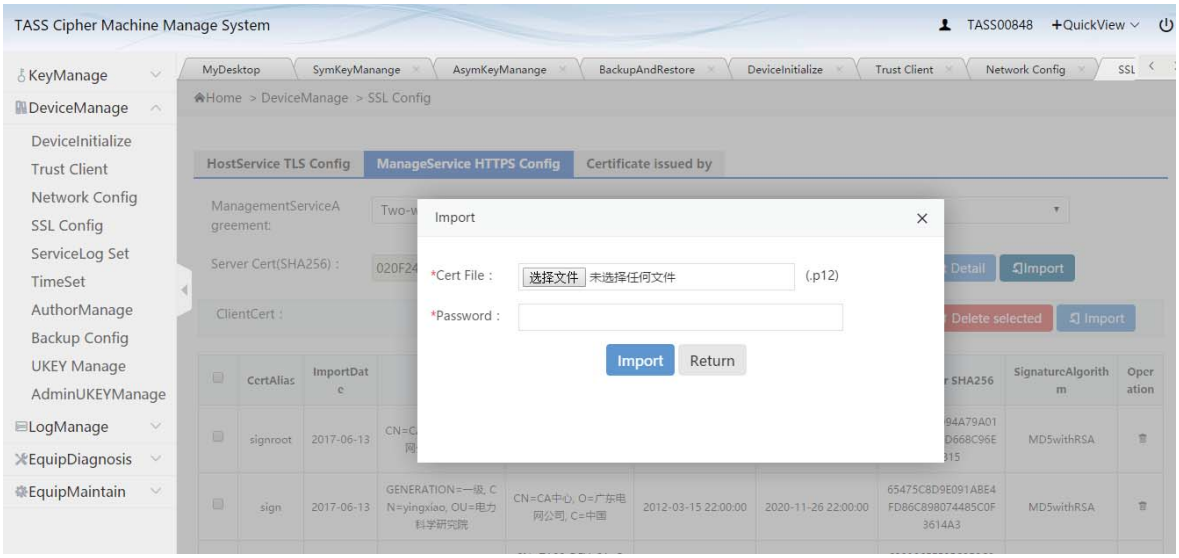
Bi-directional TLS: if there is no service end certificate or no CA certificate in the device, failure to save the configuration;)

1.4.4.2. Manage The Service HTTPS Configuration



Manage the service HTTPS configuration

One. Import updates (service side certificates)

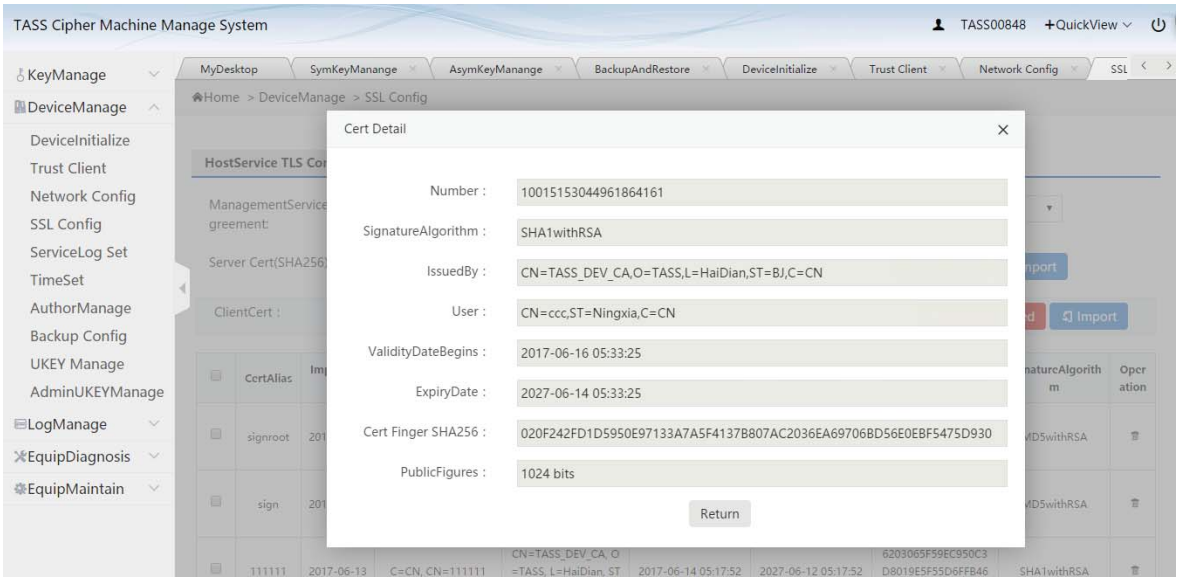


Import updates (service side certificates)

1. Certificate file: optional (p12 form certificate file);
2. Certificate private key: must be completed;

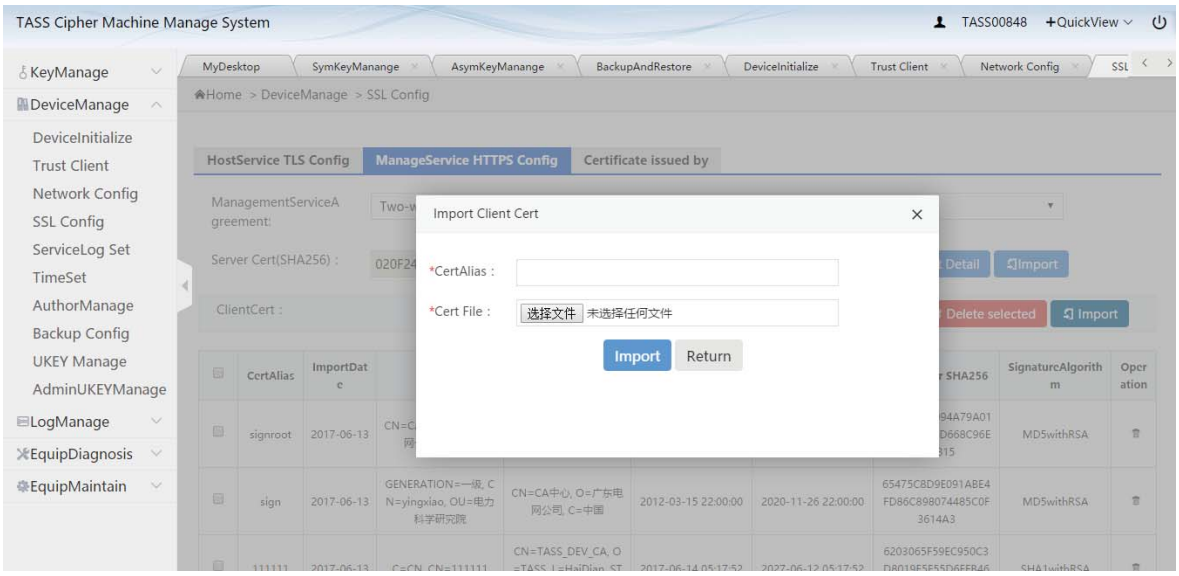
Note: after this operation is completed, the password machine should be restarted.

Two. Certificate details (client certificate)



Certificate details (service side certificates)

Three. Import (client certificate)



Import (client certificate)

1. Certificate alias: must be completed;
2. Certificate file: optional (certificate file in cer form);

Four. Delete (client certificate)

Click "delete" button or "delete" icon to execute client certificate delete.

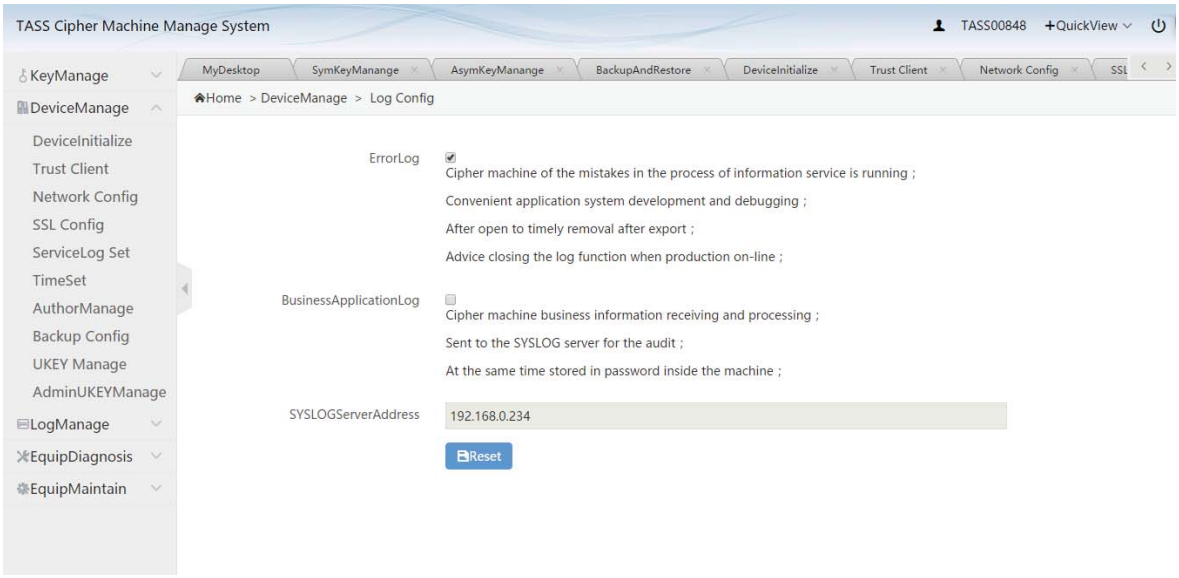
Five. Save config

Host service protocol: optional（

One-way HTTPS: failure to save the configuration if there is no service end certificate in the device;

Two-way HTTPS: if there is no service end certificate or no CA certificate in the device, failure to save the configuration;）

1.4.5. Service Log Configuration

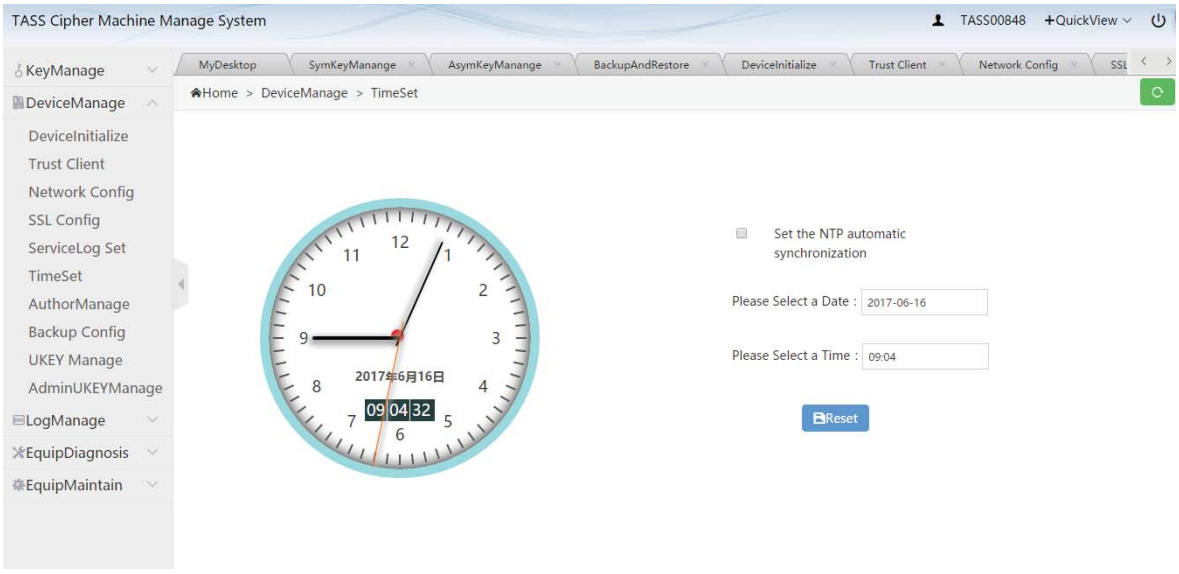


Service log configuration

1. Error logging: optional;
2. Business journal: optional;
3. SYSLOG server address: can be filled (only if the business logs have been selected);

1.4.6. Time Allocation

Method one: NTP automatically synchronizes

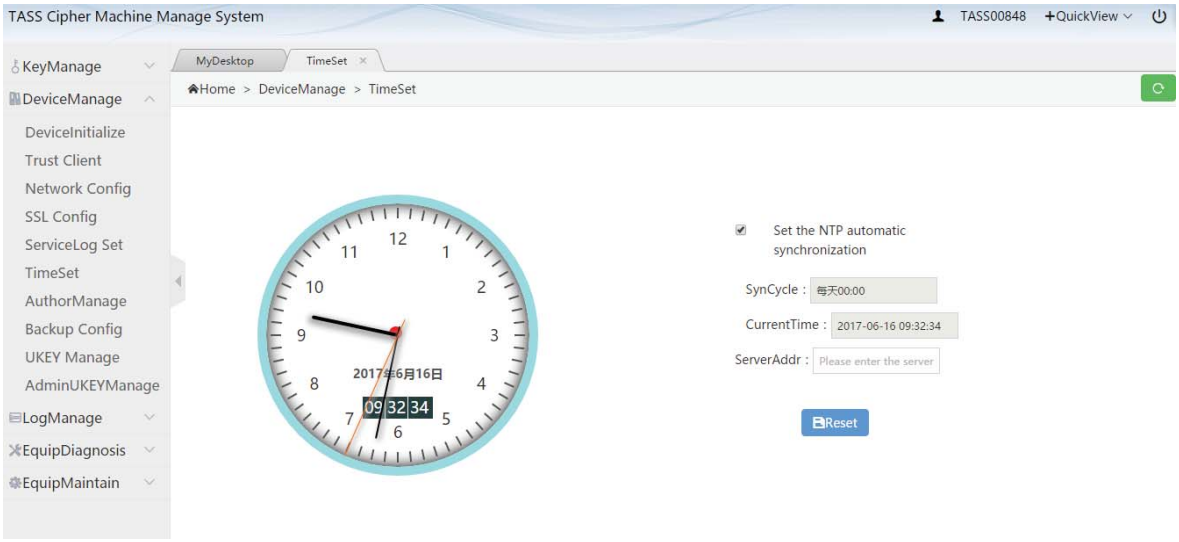


Time configuration - no NTP synchronization is set

This configuration can be reset, and the main operations are as follows:

1. Set the NTP to synchronize automatically: no.
2. ； Please select the date: reset;
3. Choose time: resets;

Method two: set the NTP to synchronize automatically

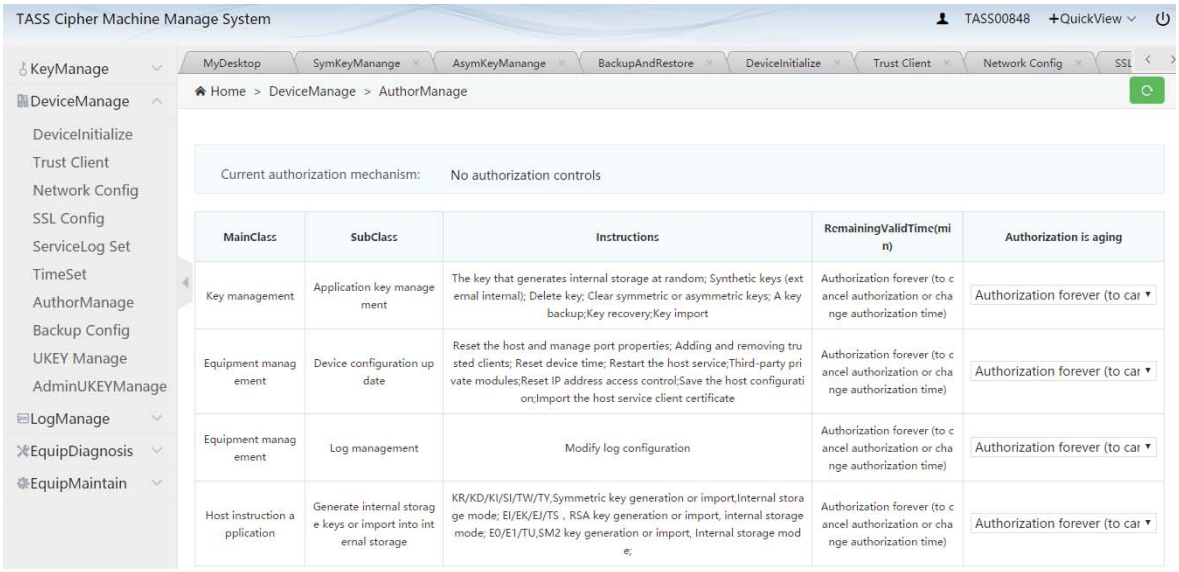


Time configuration - sets the NTP synchronization automatically

1. Set the NTP to synchronize automatically: must be selected;
2. Server IP: required;
3. This configuration is reconfigurable: when you select the "NTP automatic synchronization" button, the server time will synchronize the time that the domain server IP is located.

1.4.7. Authorization Management

First, there is no authorization mechanism



Authorization management - no authorization mechanism

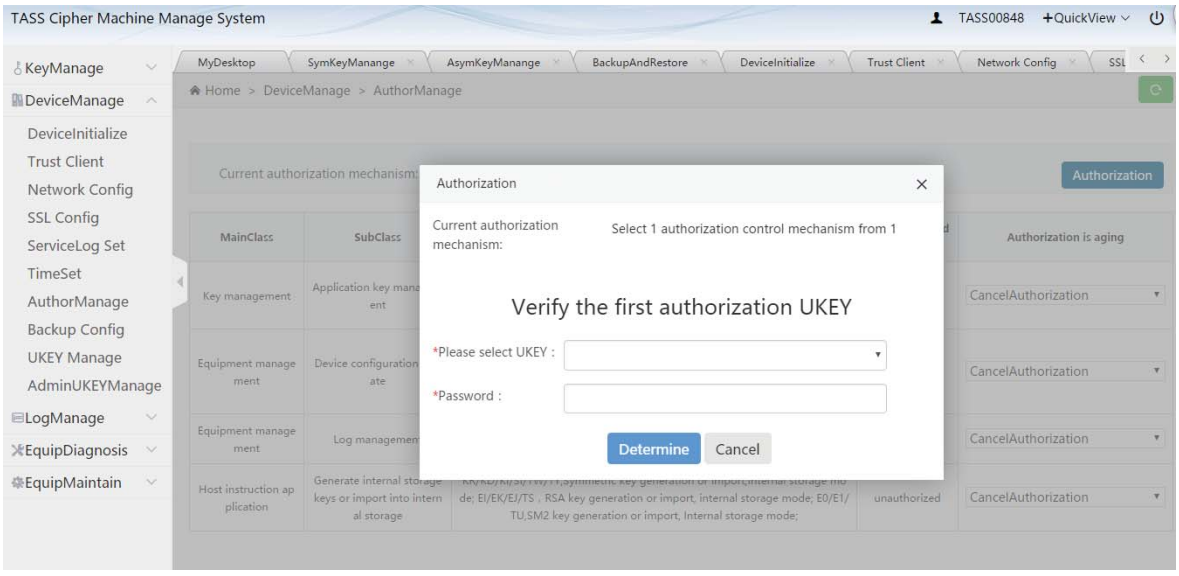
Second, there is the empowerment mechanism

Authorization management list - authorized mechanism

Note: 1. Select the information in the "action" column and grant authorization.

2. Click the "authorization" button, first to authorize UKEY validation;

1.4.7.1. Authorization

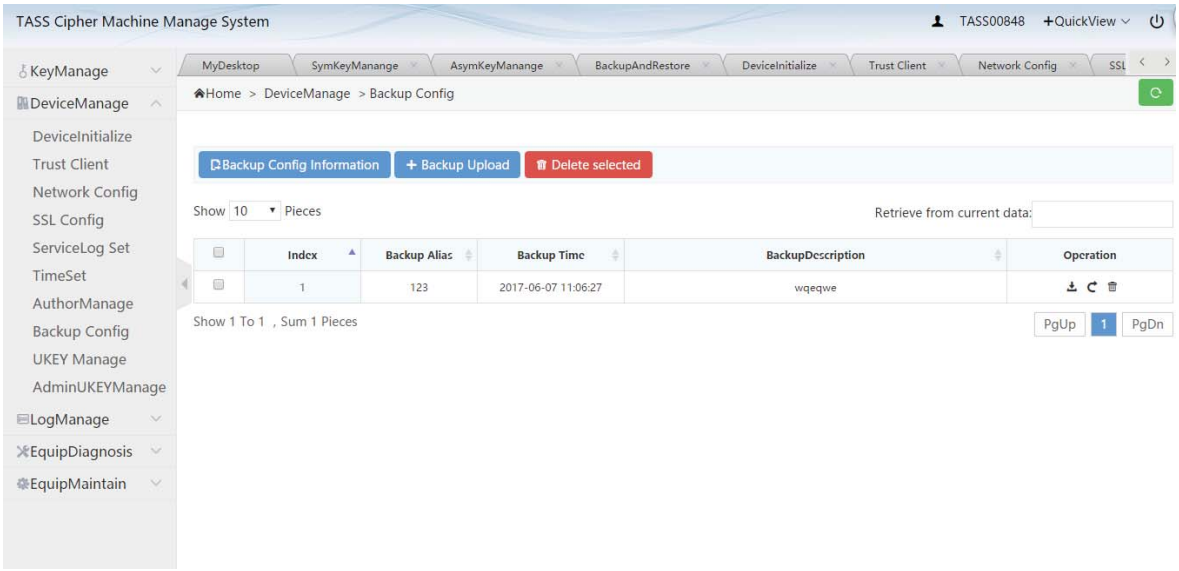


Authorized Ukey validation

1. Please select UKEY.
2. UKEY password: must be filled;

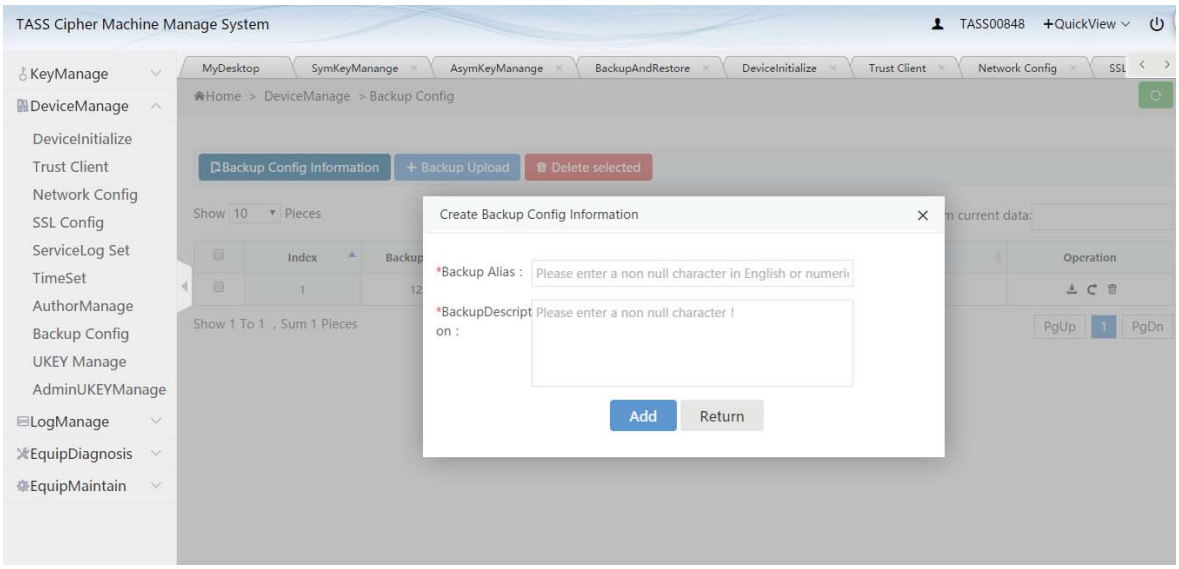
Note: after the authorization UKEY validation is completed, the system will be automatically authorized according to the selected authorization mode.

1.4.8. Configure Backup



Configure the backup list

1.4.8.1. Backup Configuration Information



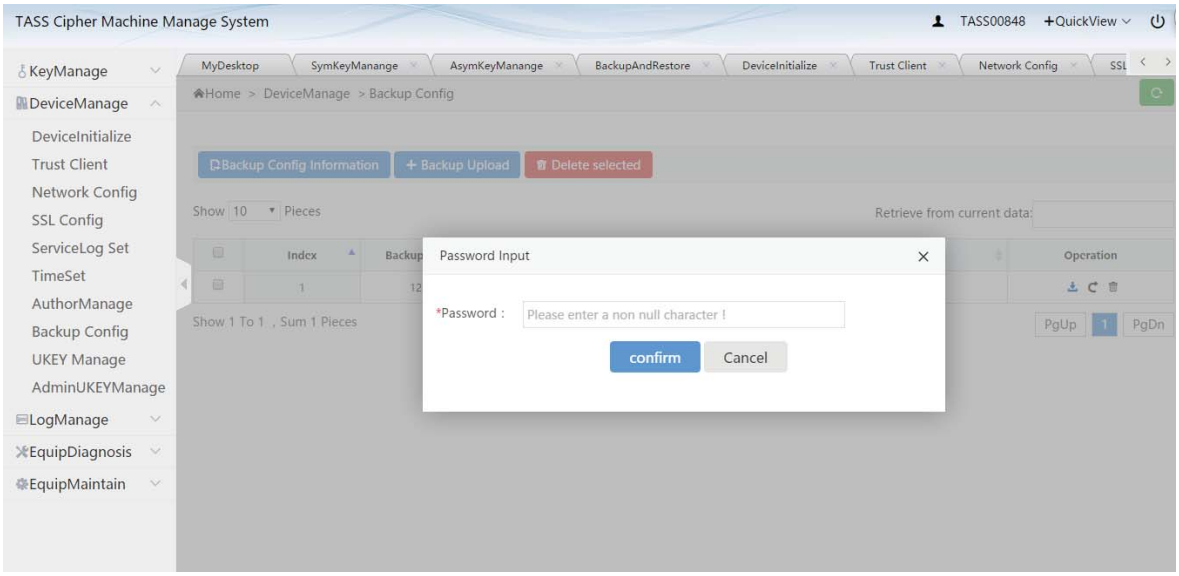
Backup information configuration

1. Backup alias: must be filled;
2. Backup instructions: mandatory;

When the "add" button is clicked, the information is packaged and saved.

- Password machine service configuration information /tapki/cfg/devcfg.ini, client.ini, Third party module certificate file；
- Host service SSL's CA/client certificate, database/tapki/db/hsmkey.sql table hostClientCert_info;
- Manage service SSL client certificate, / home/SSL/webmngclient keystore file;

1.4.8.2. Download The Backup

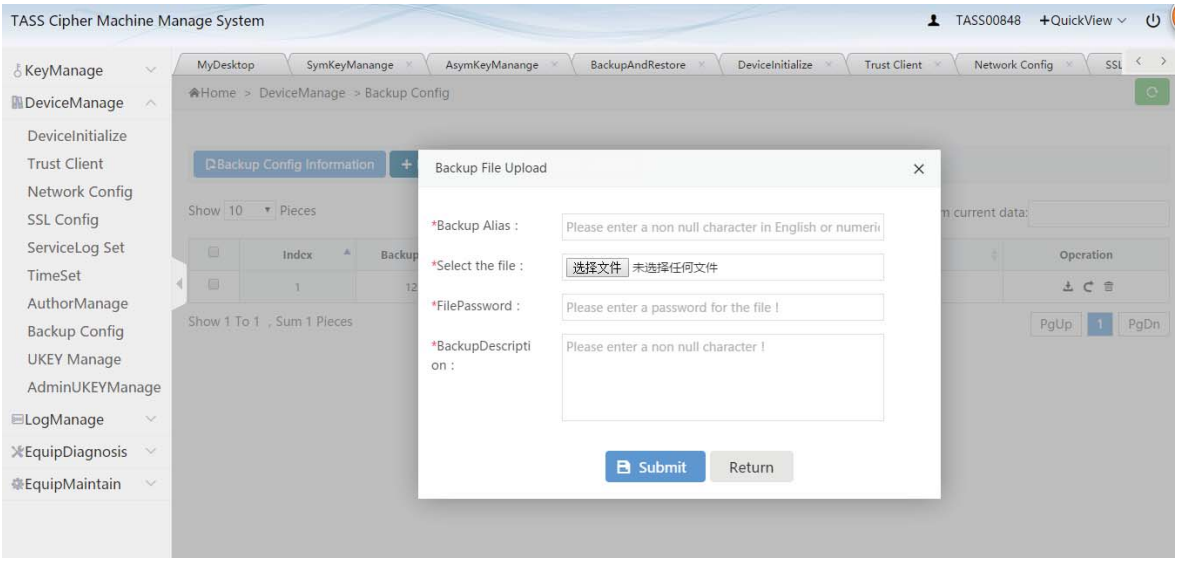


Download the backup

Protection password: must be filled (you need to set up a protection password for uploading a backup password.)

When you click the "ok" button, the system will find the created backup archive archive and download it.

1.4.8.3. Backup To Upload



Backup to upload

1. Backup alias: must be filled;
2. Select file: you will choose the backup file that you created and downloaded (zip zip file).
3. File password: must be filled in. This password should be consistent with the protection password that the administrator installed when downloading the backup.
4. Note: must be completed;

When the "submit" button is clicked, the selected backup package file is uploaded.

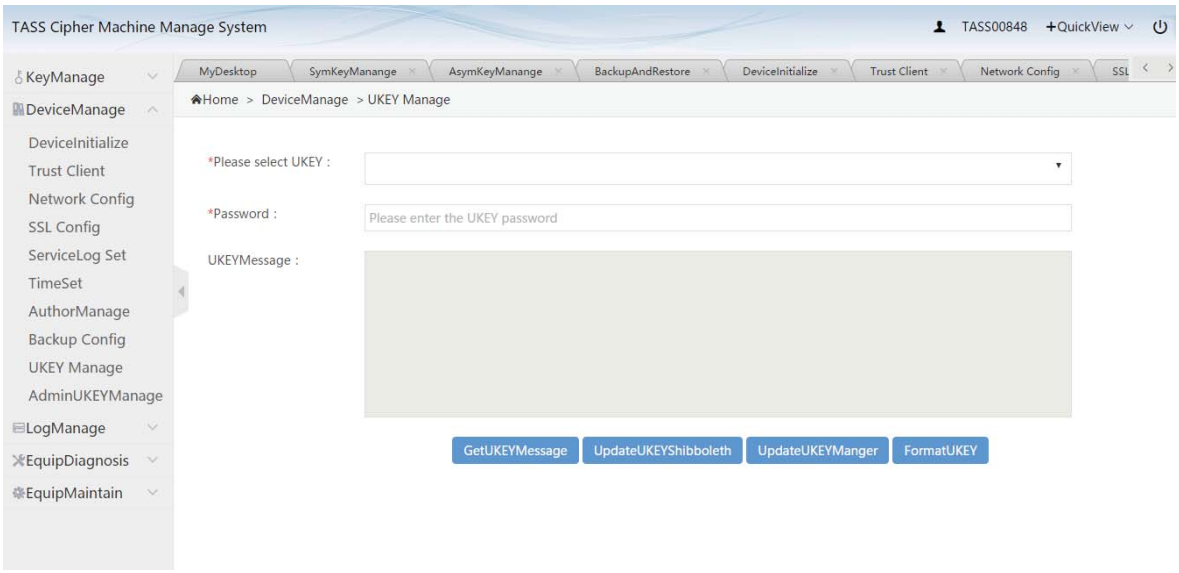
1.4.8.4. Backup Recove

When the "backup restore" icon is clicked, the backup content is decompressed and the original configuration file is overridden (consider IP addresses, etc.).

1.4.8.5. Backup Delete

Click the "delete backup" button or "delete" icon, deleting the backup document that the user created or uploaded.

1.4.9. UKEY Manager



UKEY manage

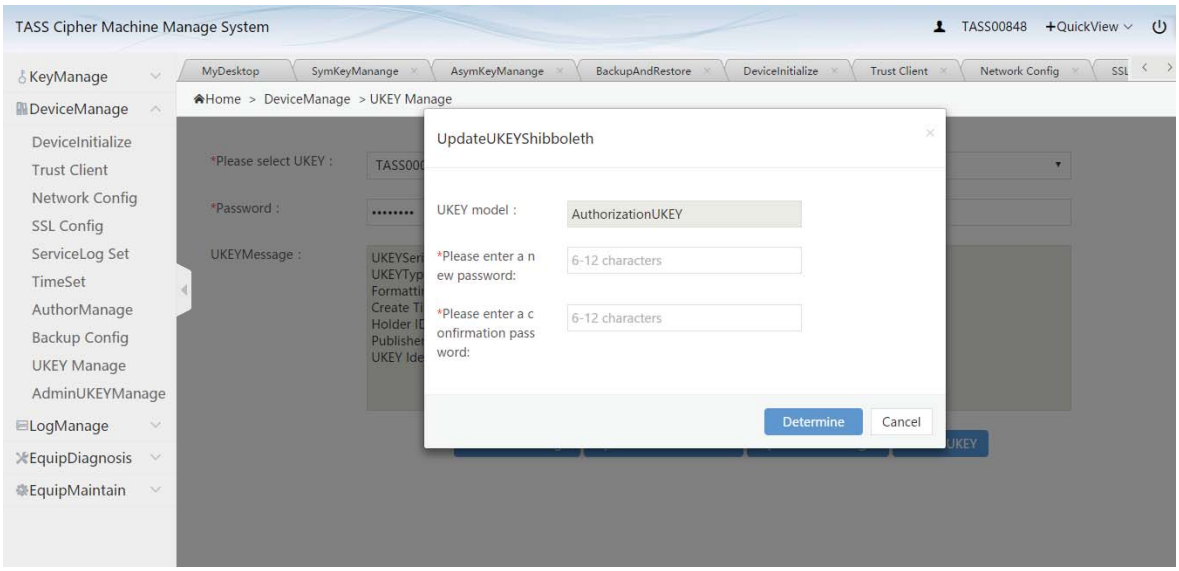
1.4.9.1. Get The UKEY Information

1. Please select UKEY.
2. UKEY password: must be filled;

Click the "get the UKEY info" button, and in the UKEY information column, you will display the basic UKEY information.

1.4.9.2. Change The UKEY Password

Before this operation is executed, you must select the UKEY and enter the UKEY password.

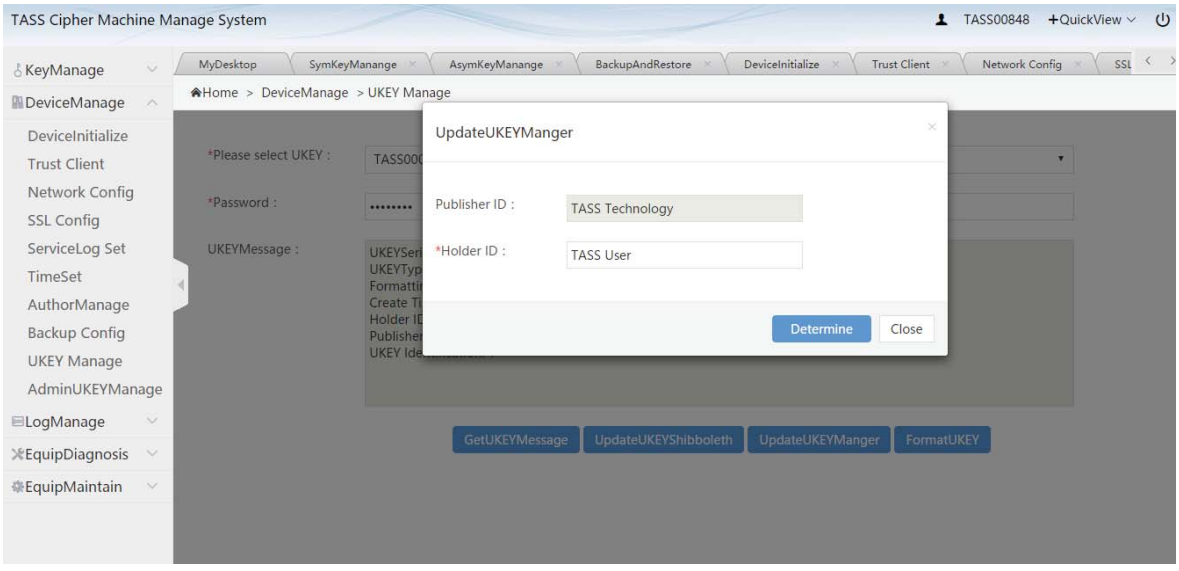


Change the UKEY password

1. Please enter the new password: must fill.
2. Enter the new password again: must fill (the same);

1.4.9.3. Modify The UKEY Information

Before this operation is executed, you must select the UKEY and enter the UKEY password.



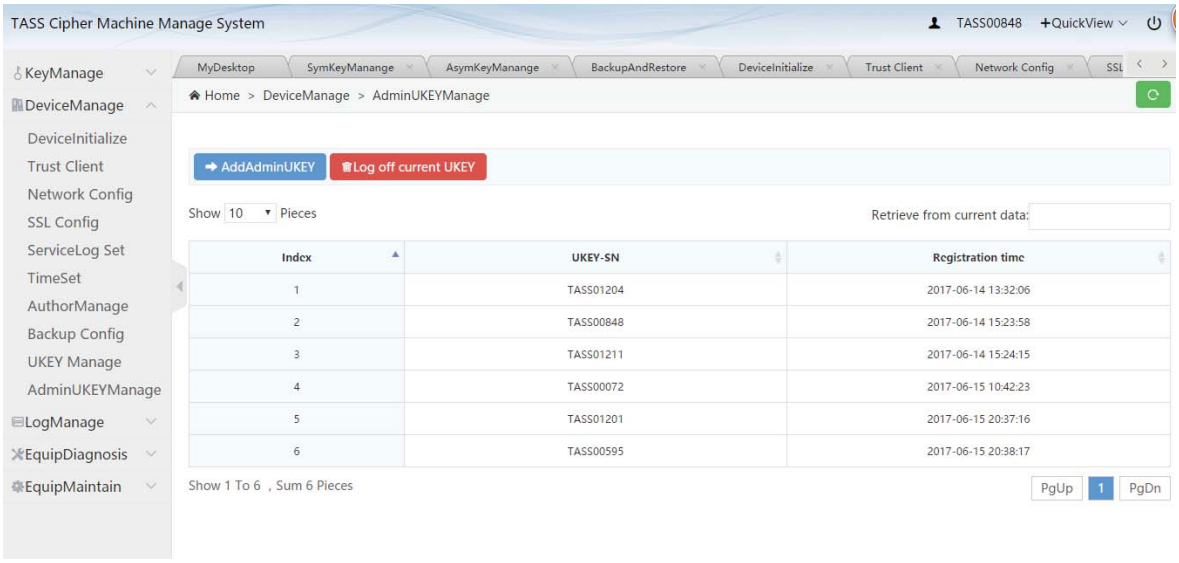
Modify the UKEY information

1. Possessor: yes

1.4.9.4. Format The UKEY

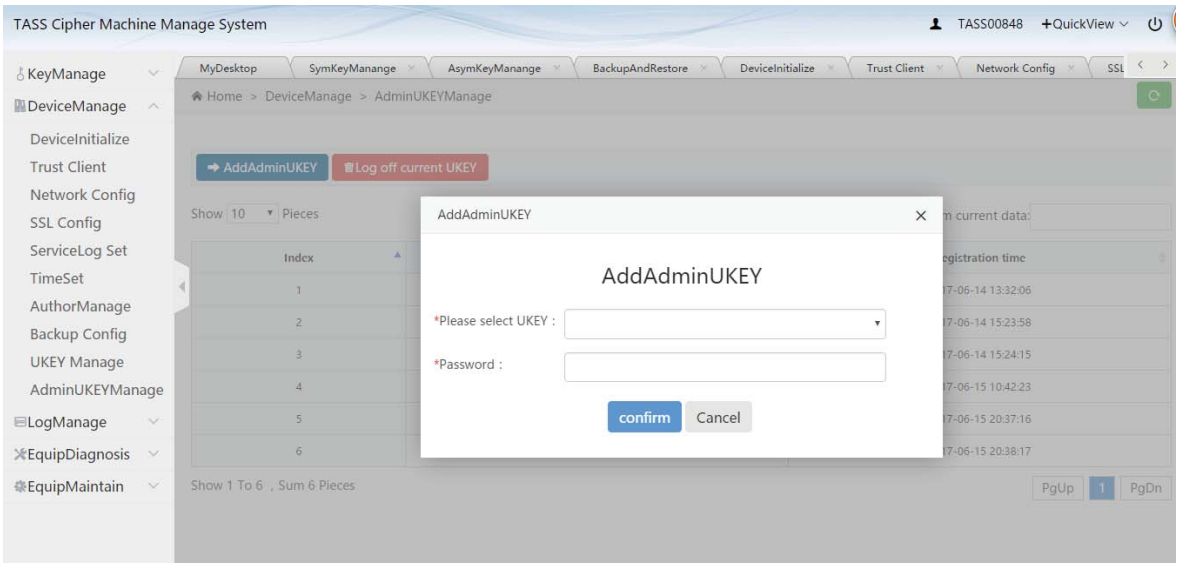
Formatting UKEY: click "formatting" to format the UKEY information.

1.4.10. Administrator UKEY Management



Administrator UKEY management

1.4.10.1. Add The Administrator UKEY



Add the administrator UKEY

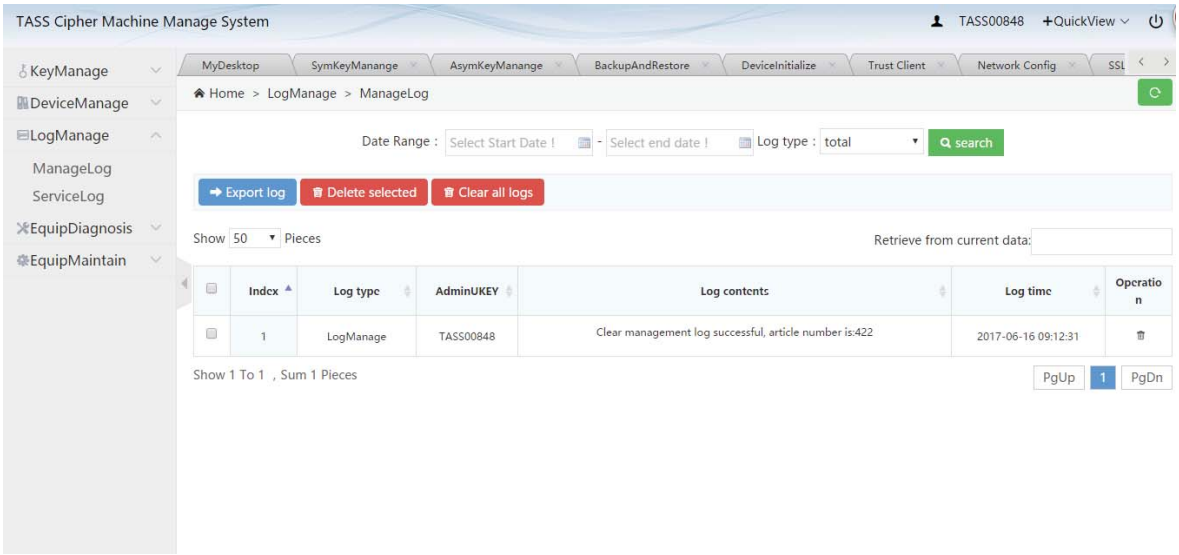
1. Please select UKEY.
2. UKEY password: must be filled;

1.4.10.2. Log Out The Current Administrator

Log out the administrator UKEY that is logged in

1.5. Log Manage

1.5.1. Manage Log



Management log list

The management log list is a display of existing log messages and executable actions.

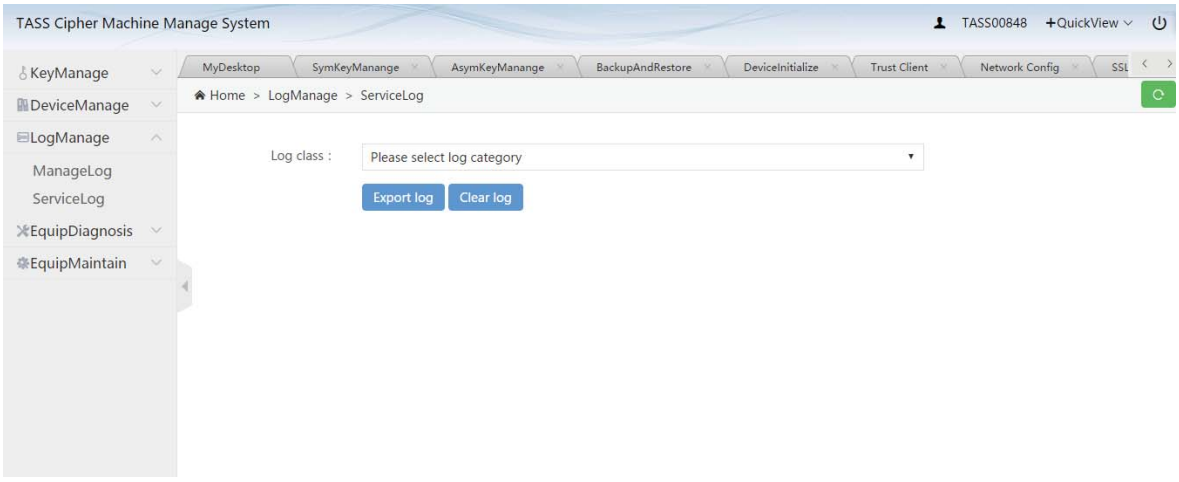
1.5.1.1. Export Log

When you click the export Log button, you will export the management log list to the Excel table;

1.5.1.2. Delete

Click the "clear selected" button or "clear all log" icon to perform the deletion or emptying of the management log;

1.5.2. Service Log



Service Log

1.5.2.1. Export Log

Log categories: required;

When you click the export Log button, the service log is exported to the log file.

1.5.2.2. Clear Log

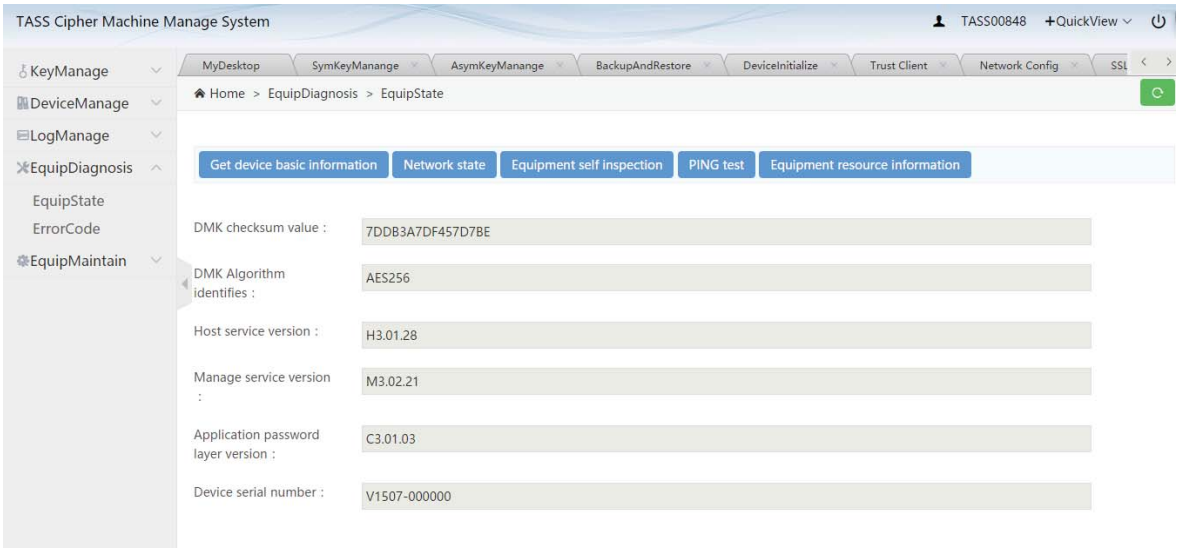
Log categories: required;

Click the clear Log button to perform cleanup operations on the service log.

1.6. Equipment Diagnosis

1.6.1. Equip State

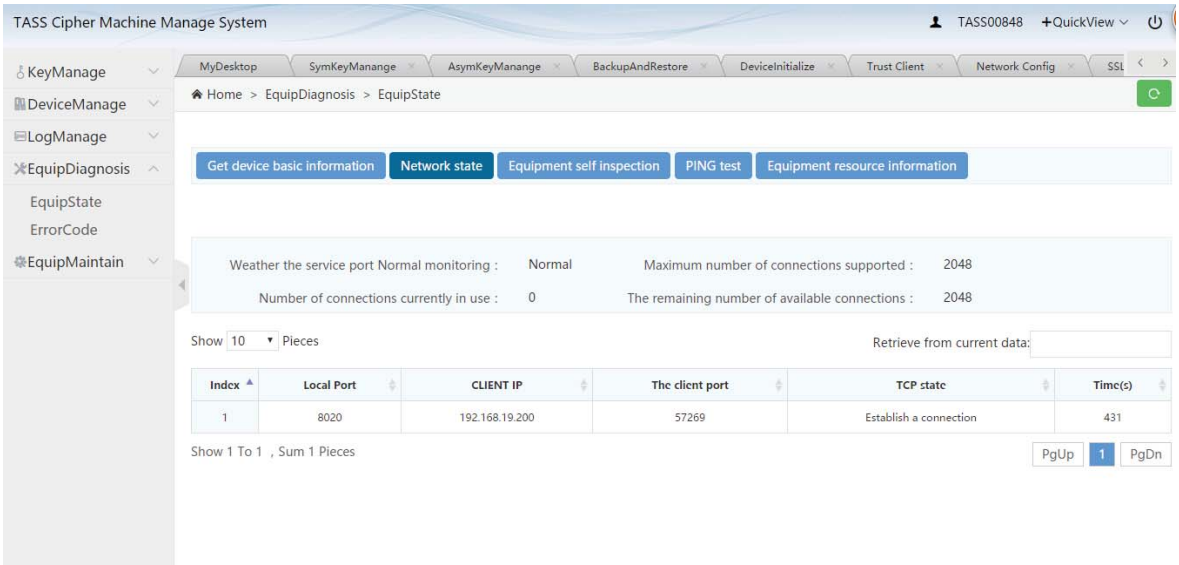
1.6.1.1. Get Ddevice Basic Information



Device base information

Equipment basic information display.

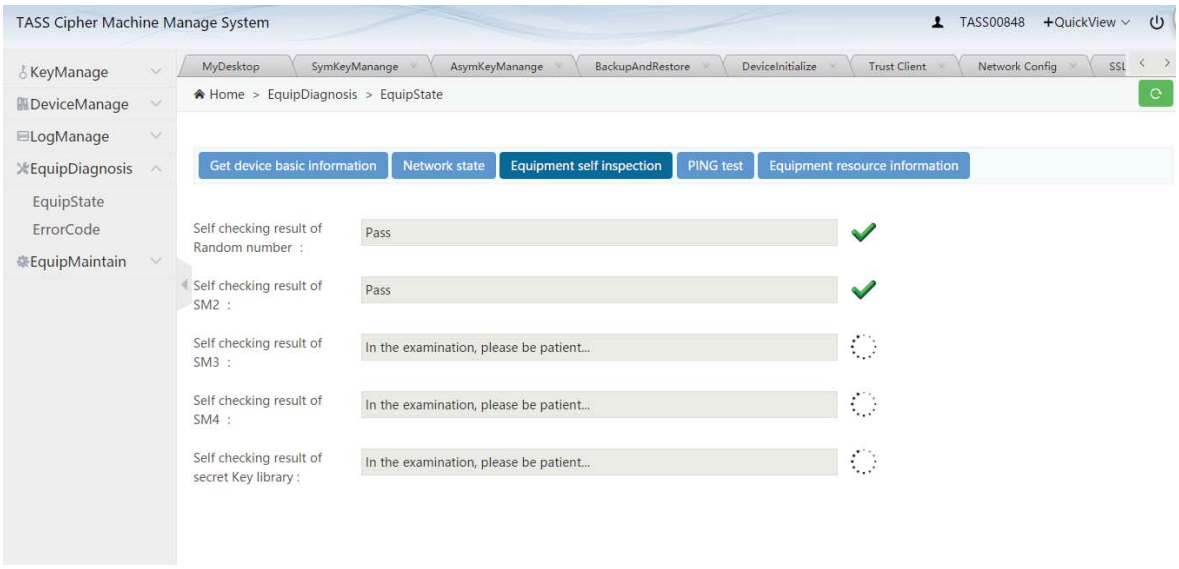
1.6.1.2. Network State



Network state

Network status display.

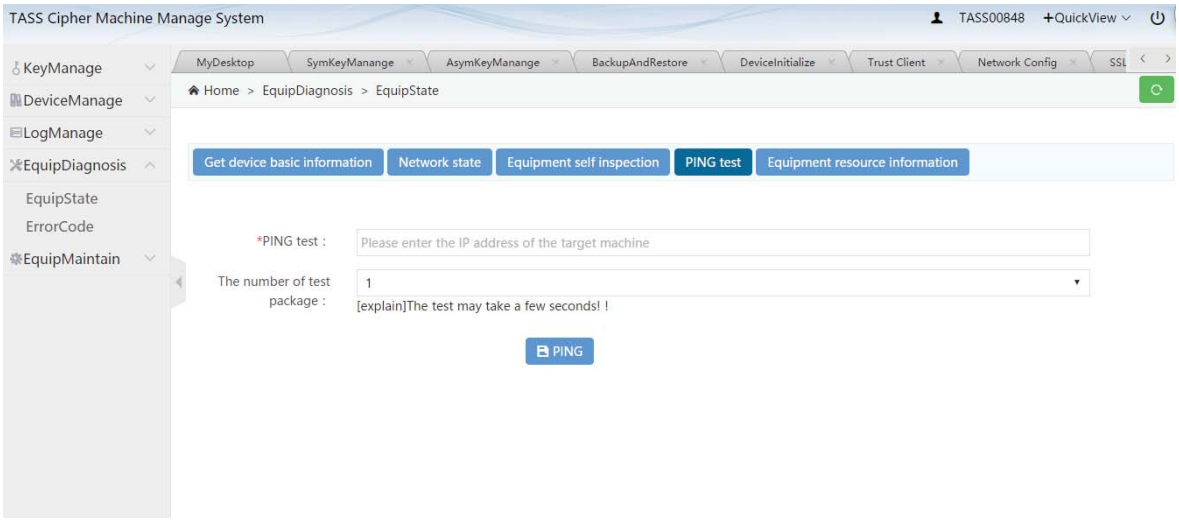
1.6.1.3. Equipment Self Inspection



Equipment self inspection

Equipment self inspection result display.

1.6.1.4. PING Test



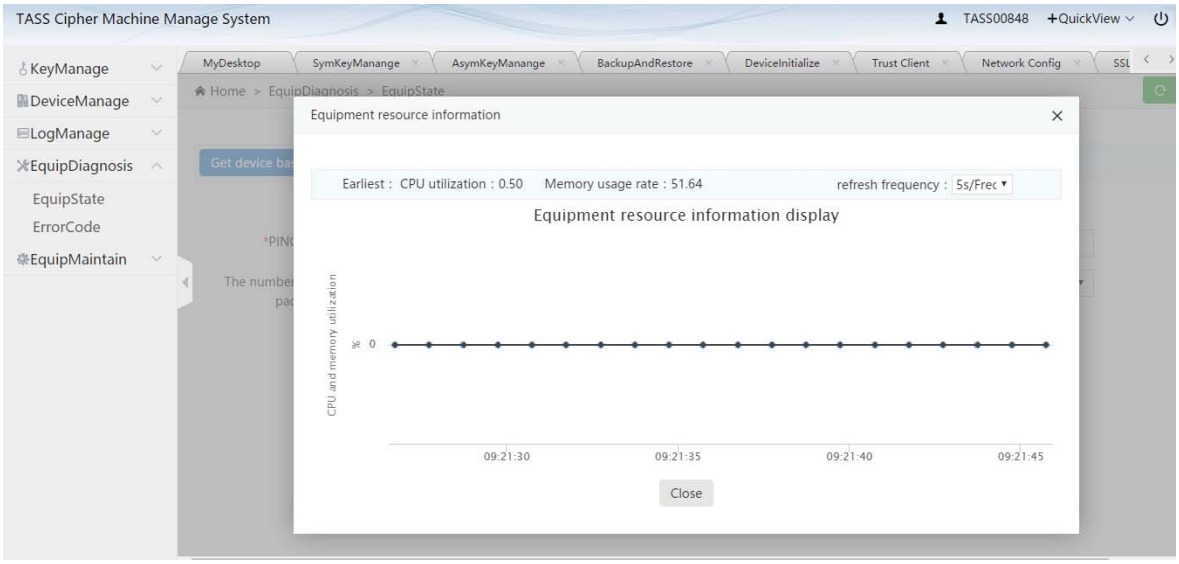
PING Test

1. Target IP address:required(IP to test);

2. Number of test packages:required;

3. When you click the PING button, the system prompts the number of responses to the package. If 0, the PING test does not pass;

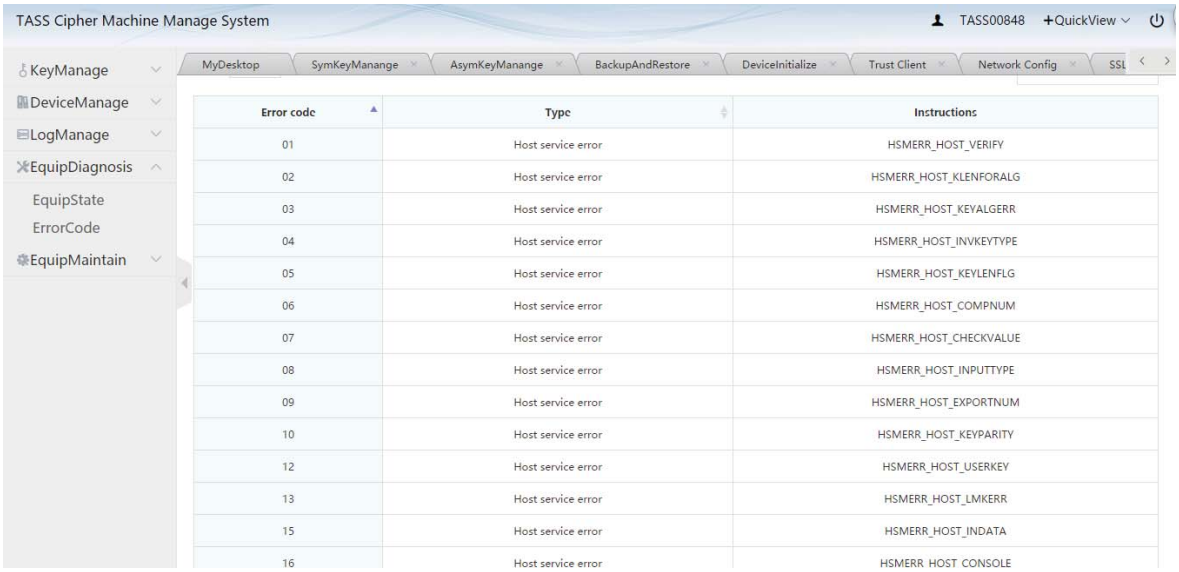
1.6.1.5. Device Resource Information



Device resource information

Equipment resource information use status display, optional dynamic display frequency 5s/ times or 10s/ times.

1.6.2. Error Code

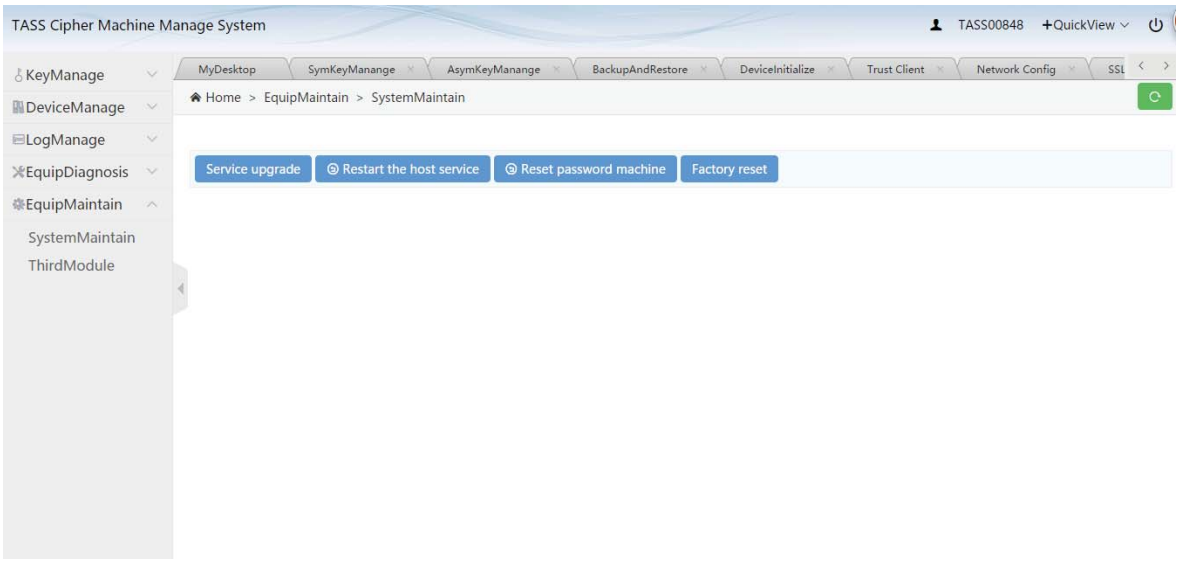


Error code list

The error code list is a display of the error code information of the existing cryptographic machine and supports the fuzzy query.

1.7. Equip Maintain

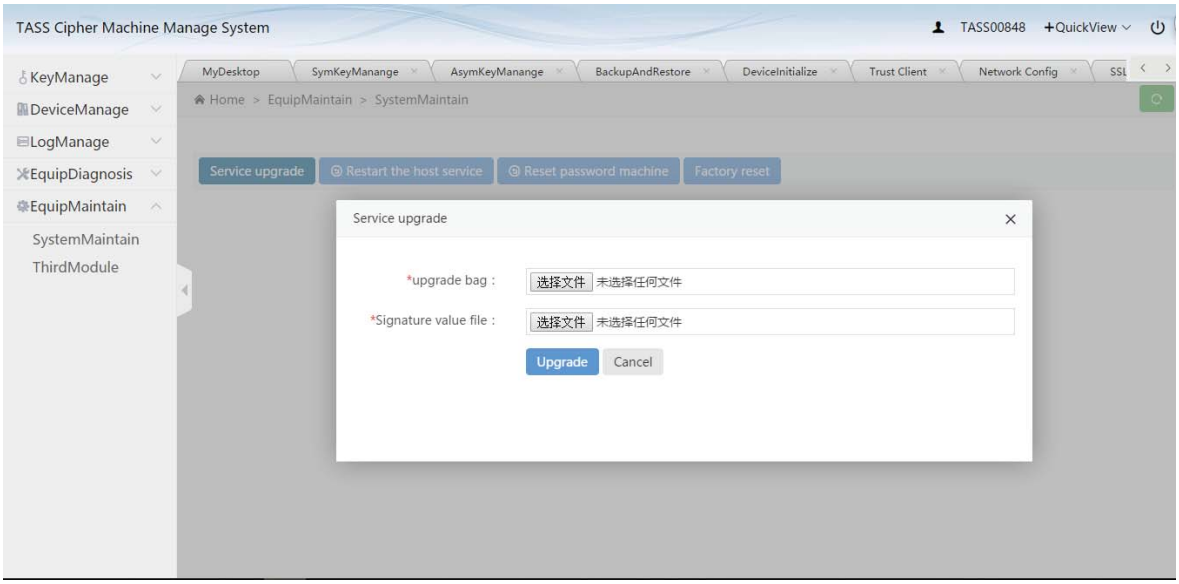
1.7.1. System Maintain



System Maintain

System maintenance is mainly for the whole system upgrade, restart and restore factory settings and other operations;

1.7.1.1. Service Upgrade

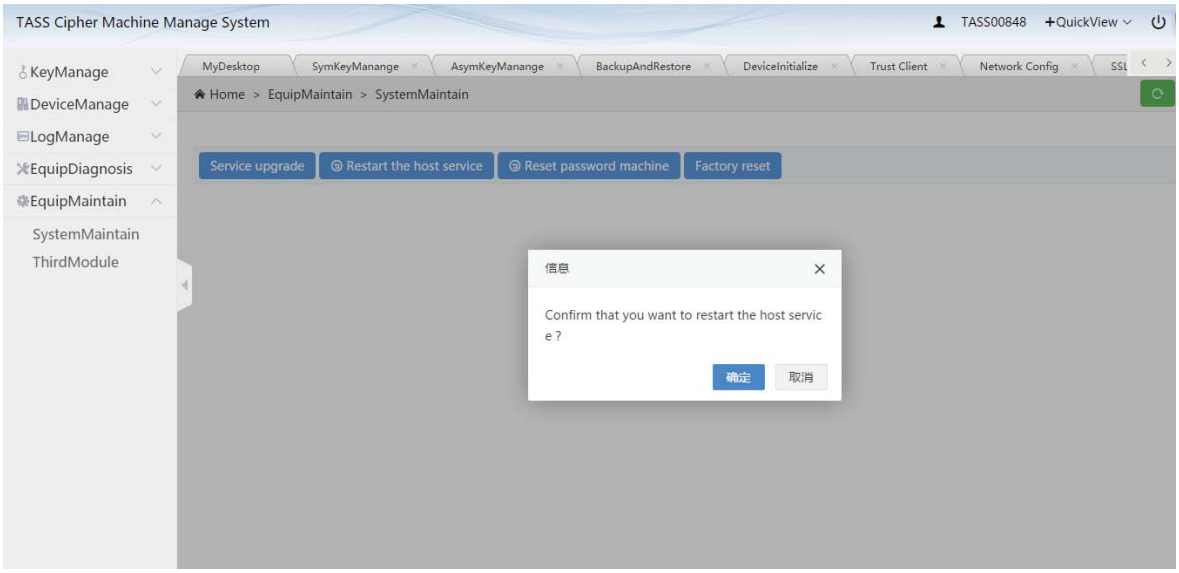


Service upgrade

1. Upgrade package: required;
2. Signature value file: required;

Be careful：After this operation, the host service needs to be restarted before it becomes effective.

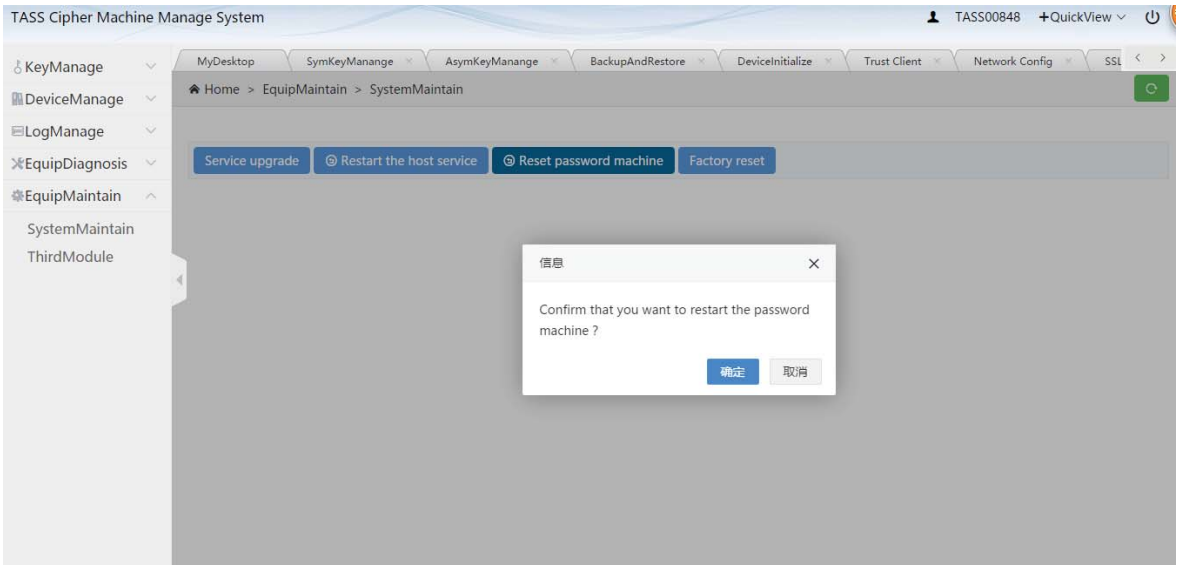
1.7.1.2. Restart The Host Service



Restart the host service

When you click the restart host service button, the system will indicate whether the reboot is prompted and the host service will restart after confirmation.

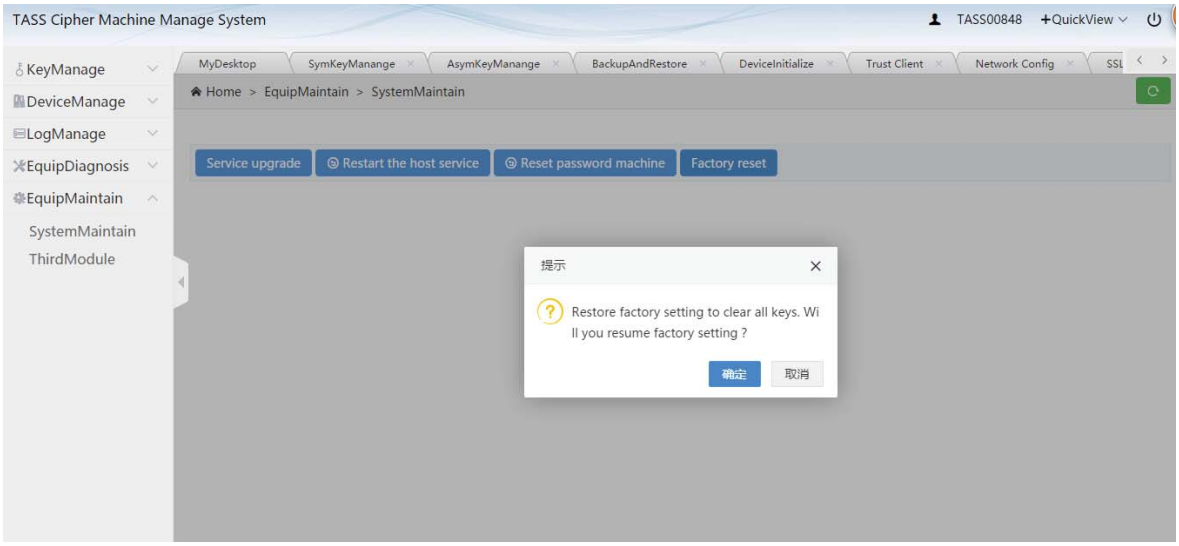
1.7.1.3. Restart Password Machine



Restart password machine

Click the "restart password machine" button, the system will be given whether to restart the prompt, confirmed that the password machine will restart.

1.7.1.4. Factory Reset



Factory reset

Click the "restore factory settings" button, the system will be given whether to restart the prompt, confirmed that the password machine will resume factory settings.

Restore factory settings, the system will automatically perform operations:

1.Empty all keys in the crypto machine;

2.Load test master key;

3.The reset authorization mechanism is the model without authorization mechanism;

4.Clear all trusted clients;

5.SSL configuration and certificate reset;

6.Service port property reset;

7.Clear third party modules and certificates;

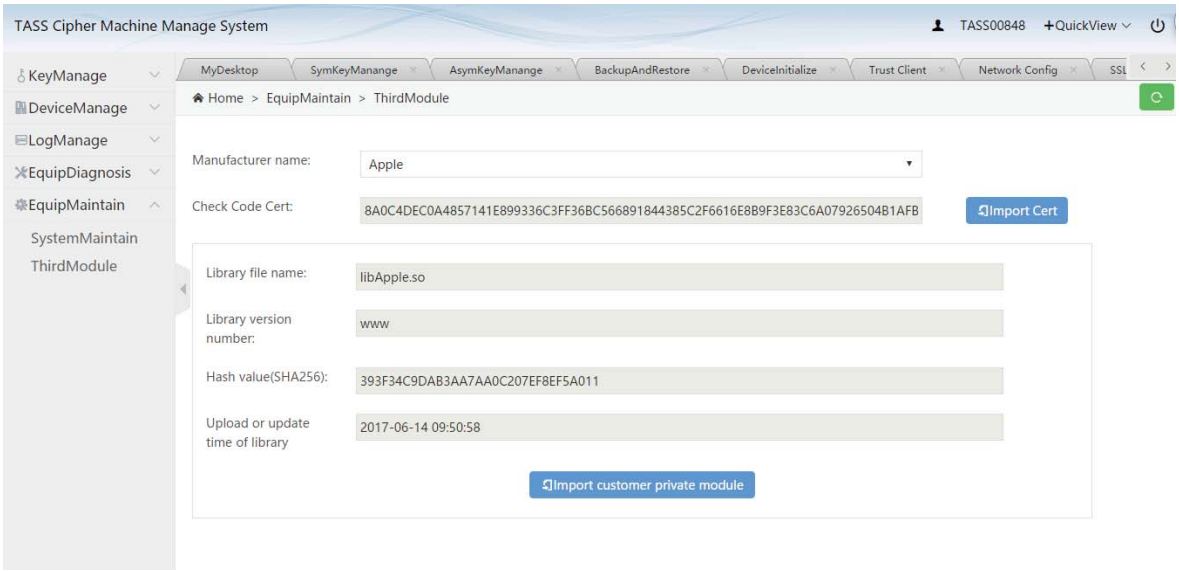
8.Reset service log;

9.Empty administrator information;

10.Empty the backup configuration table and delete the backup file;

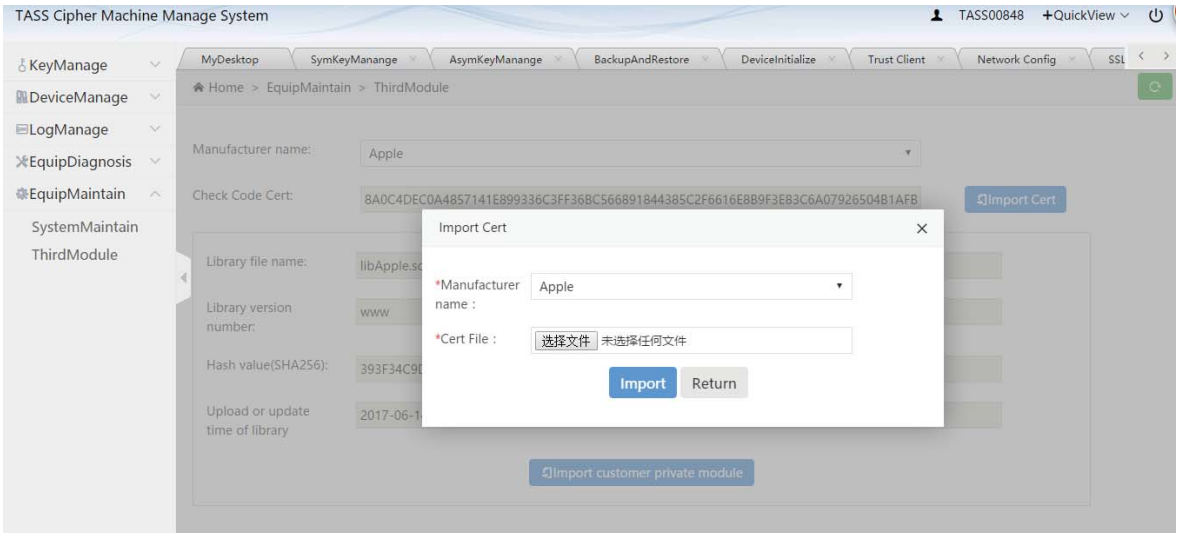
Tip: Please operate carefully!

1.7.2. Third Module



Third Module

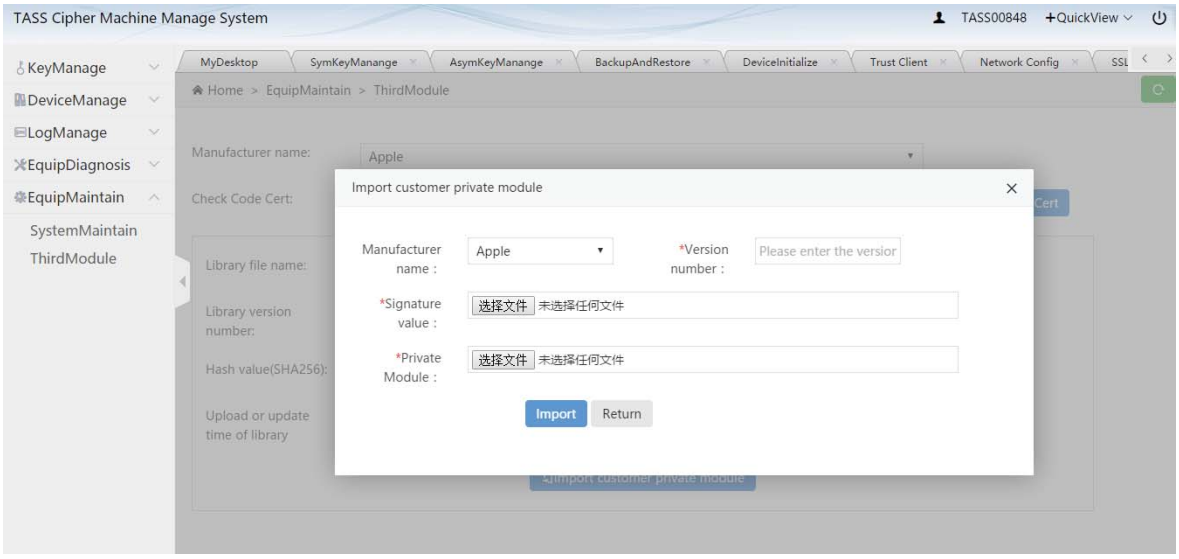
1.7.2.1. Import Third Party Certificates



Import third party certificates

1. Manufacturer name: Required;
2. Certificate file: Required;

1.7.2.2. Import Client Private Module



Import Client Private Module

Notice: Before you do this, you must import the third party certificate. After this operation, the host service needs to be restarted before it becomes effective.

1. Manufacturer name: Required;
2. Version number: Required;
3. Signature value: Required;
4. Private module: Required;

2. PASSWORD MACHINE SERIAL PORT COMMAND INSTRUCTIONS

When IP is unknown, the cipher machine can be connected through the serial port.

2.1. Introduction Of Serial Terminal Connection

The serial port is used to connect the management panel of the back panel of the encryption machine. The port number, baud rate 115200, data bit 8, stop bit 1, parity check none are selected in the remote terminal. Then enter enter, with the following prompt for login success:

Last login: Mon Jun 5 11:36:51

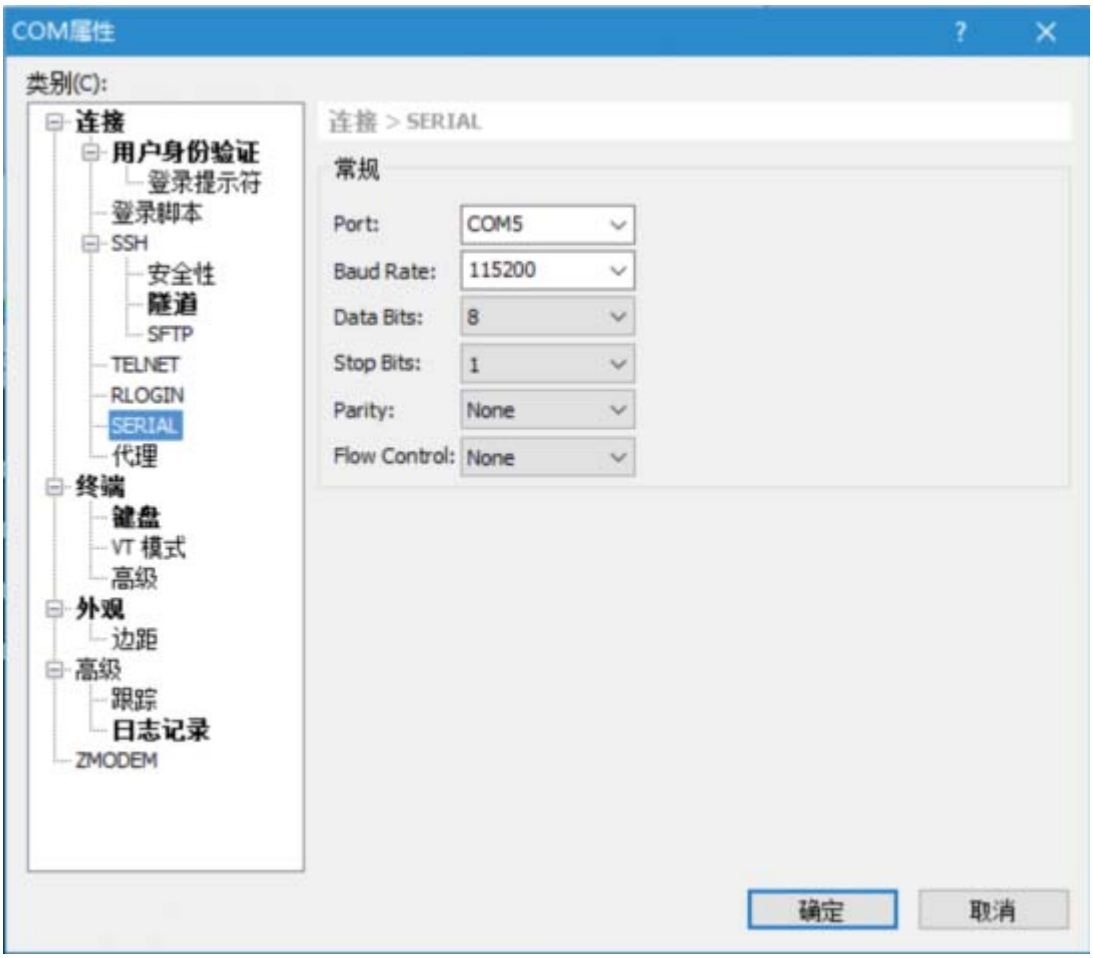
Hsm >

2.1.1. Serial Login

1、View port numbers (take win10 as an example)

This computer management (Computer - > right) - > device manager > port

Take xshell for example:



2、Display serial command

Enter the Tab key to return the current command supported by the serial port.

Hsm >Tab

cm exit ping qm reset

Hsm >

2.2. Exit

Use: exit the terminal serial interaction.

How to use: exit

Example:

Hsm >exit

Then you need to turn off the terminal and re-enter.

2.3. Ping

Purpose: test network connectivity.

How to use: Ping enter, and then press the prompt to enter the network address you want to test.

Example:

Hsm >ping

Please enter the address you want to test:192.168.19.200

PING 192.168.19.200 (192.168.19.200) 56(84) bytes of data.

64 bytes from 192.168.19.200: icmp_seq=1 ttl=64 time=0.015 ms

64 bytes from 192.168.19.200: icmp_seq=2 ttl=64 time=0.019 ms

Ctrl+c exit

2.4. Qm

Purpose: check the current network configuration of this machine.

How to use: qm enter

Example:

Hsm >qm

Management service address:192.168.19.200

Management service mask:255.255.255.0

Management service gateway:192.168.19.254

Hsm >

2.5. Cm

Purpose: modify the network configuration of this machine.

How to use: cm enter, and then press the prompt to enter the relevant network parameters.

Example:

Hsm >cm

Enter network address(current：192.168.19.200)：192.168.19.201

Enter the gateway address(current：192.168.19.254)：192.168.19.254

Input subnet mask(current：255.255.255.0)：255.255.255.0

Configuration successful, restart HSM effective

Hsm >

Restart effect.

2.6. Reset

Purpose: restore factory settings.

How to use: reset enter, and then press the prompt operation.

Example:

Hsm >reset

Warning: this operation will clear all keys in the password machine. Do you want to continue?[Y/N]:y

Turn the safety status lock to safe condition and press enter:

The encryption machine is in safe mode!

Clear DMK and user keys... Success!

Clear third party modules and certificates... Success!

Load test master key... Success!

Reset licensing mechanism... Success!

SSL configuration and certificate reset... Success!

Clear all trusted client addresses... Success!

Service port property reset... Success!

Reset system configuration... Success!

Clear backup configuration data tables and configuration files... Success!

Reset to factory settings, please restart the system!

Hsm >

Restart the machine.

Remarks: the above command output prompt shows that the character set is UTF-8. If there is a garbled code, the character set of the terminal needs to be adjusted.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-- Reorient or relocate the receiving antenna.

-- Increase the separation between the equipment and receiver.

-- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-- Consult the dealer or an experienced radio/TV technician for help.